EXHIBIT 1

Ekwan E. Rhow - State Bar No. 174604
erhow@birdmarella.com
Marc E. Masters - State Bar No. 208375
mmasters@birdmarella.com
~~Oliver Rocos - State Bar No. 319059~~
~~*orocos*~~*@birdmarella.com*
BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100

Jonathan M. Rotter - State Bar No. 234137
jrotter@glancylaw.com
David J. Stone - State Bar No. 208961
dstone@glancylaw.com
GLANCY PRONGAY & MURRAY LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150
Email: info@glancylaw.com

Korey A. Nelson (~~to be~~ admitted *pro hac vice*)
knelson@burnscharest.com
Amanda K. Klevorn (~~to be~~ admitted *pro hac vice*)
aklevorn@burnscharest.com
Claire E. Bosarge (~~to be~~ admitted *pro hac vice*)
cbosarge@burnscharest.com
BURNS CHAREST LLP
365 Canal Street, Suite 1170
New Orleans, LA 70130
Telephone: (504) 799-2845

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

GRACE LAU~~and~~, CHRISTOPHER KARWOWSKI, MELODY KLEIN, MICHAEL MCBRIDE, and AIMEN HALIM, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

GEN DIGITAL INC., a corporation, and

CASE NO. ~~4~~:22-cv-08981-JST

FIRST AMENDED CLASS ACTION COMPLAINT FOR:

1. **Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510~~,~~ *et seq.***
2. **Violation of the California Invasion of Privacy Act, California Penal**

Style Definition: Footnote Text,Char,Footnote Text Char Char,Footnote Text Char Char Char Char Char Char,Footnote Text Char Char1 Char Char,Footnote Text Char1,Footnote Text Char1 Char Char Char Char,Footnote Text Char2 Char Char: Font:

Formatted: Font: Italic

Formatted: Font color: Auto

Formatted: Font: Not Italic

Formatted: Line spacing: single

Formatted: Line spacing: single

Formatted: Line spacing: single

Formatted: Font: Italic

Formatted: Line spacing: single

JUMPSHOT INC., a corporation,

Defendants.

Code §§ 631 and 632

~~*(caption continued on next page)*~~

3. **Violation of the Right to Privacy - California Constitution**
4. **Intrusion upon Seclusion**
5. **Statutory Larceny, California Penal Code §§ 484 and 496**
6. **Violation of the California Unfair Competition Law, Bus. & Prof. C. §§ 17200 *et seq.***
7. **Unjust Enrichment**

DEMAND FOR JURY TRIAL

Formatted: Line spacing: single

Formatted: Font: Italic

Formatted: Font: Bold, No underline

Formatted: No underline

Formatted: Line spacing: Exactly 12 pt

Formatted: Default Paragraph Font

Formatted: _Pld Footer Adjustment, Position: Horizontal: Left, Relative to: Column, Vertical: In line, Relative to: Margin, Wrap Around

Formatted: _Pld Footer Adjustment

Plaintiffs Grace Lau ~~and~~, Christopher Karwowski, Melody Klein, Michael McBride and Aimen Halim ("Plaintiffs"), individually and on behalf of ~~a class~~classes of similarly situated individuals, by and through their undersigned counsel, allege the following against Gen Digital, Inc. ("Gen Digital") and Jumpshot, Inc. ("Jumpshot" and, collectively with Gen Digital, "Defendants"), upon information and belief:

INTRODUCTION

1. This is a case about Defendants' surreptitious electronic surveillance of their customers and invasion of their customers' privacy by intercepting, collecting, ~~and~~ storing, using, and sharing customers' Internet search engine keyword searches, search results, ~~and~~ email inbox searches~~.~~, browsing histories, and video viewing histories. The private data intercepted, collected, stored, used, and shared by Defendants also includes highly sensitive protected health information ("PHI") – such as information on users' medical conditions, immunizations, allergies, and prescriptions. Defendants' wrongful ~~practice was~~practices were not disclosed to their customers.

2. What makes this present conduct even more egregious is that after Defendants engaged in similar illegal conduct in the past and were caught doing so, Defendants purported to apologize for their actions, but then secretly revived their past practices in order to continue misappropriating their customers' ~~privacy and~~private data for the sake of profits. Defendants' illegal and persistent misconduct must now be stopped once and for all.

3. Defendants' practices all violate the federal Electronic Communications Privacy Act, the California Invasion of Privacy Act, California's Unfair Competition Law, and other statutory, Constitutional, and common law privacy, data, and consumer protections.

THE SCHEME

4. Defendant Gen Digital is a computer software company, formerly known as Symantec Corp. (1982-2019) and NortonLifeLock Inc. (2019-2022). ~~-~~In 2022, it acquired the entirety of the assets of a company called Avast PLC ("Avast"). ~~-~~It is therefore Avast's successor, and it is responsible for Avast's liabilities.

5. While Avast is no longer an independent company, it continues to operate in much the same way as it did prior to its acquisition. ~~-~~Avast markets itself as a developer of certain

Formatted: Left
Formatted: Left
Formatted: Left
Formatted: _Pld Footer Adjustment

software that purportedly makes it safer and more secure for users to browse the Internet.

6. But Avast is a data harvester masquerading as a data protector.

7. At issue in this action is the Avast Online Security & Privacy (the "AOSP") browser extension for the Google Chrome and Microsoft Edge Internet browsers.

~~7.~~8. Avast claims that ~~its products~~AOSP (i) ~~prevent~~prevents third parties from surreptitiously tracking and collecting the users' browsing activity and personal information and (ii) ~~block~~blocks malicious websites that try to steal their data. But Avast does not disclose the fact that, while its software may prevent *third parties* from stealing users' data, its own software steals users' data *for Gen Digital and Avast*.

~~8. At issue in this action are two Gen Digital and Avast products, the Avast Online Security & Privacy (the "AOSP") and the Avast SafePrice ("SafePrice") browser extensions for the Google Chrome and Microsoft Edge Internet browsers.~~

9. According to Avast, AOSP protects users' privacy, secures users' browsers against online threats and phishing scams, keeps users' online activities private and anonymous, disguises users' online profile, and prevents tracking on every website the user visits. ~~SafePrice is marketed as providing the best prices, deals, and coupons while shopping online.~~

10. ~~However, both of these products~~AOSP, however, secretly ~~collect~~intercepts, collects, and ~~store~~stores the users' data in such a systematic way that ~~they~~it effectively ~~create~~creates a "live feed" of millions of users' Internet browsing data.

11. For years, Avast secretly monetized the data it intercepted, collected, and stored from AOSP ~~and SafePrice~~ by selling the data to Avast's own subsidiary, Jumpshot. Jumpshot then sold the data to its customers, including major retailers and marketers.

12. In October 2019, Avast's use of Jumpshot to monetize the data was exposed by third parties, resulting in consumer backlash and governmental scrutiny. In January 2020, Avast acknowledged its practice and shut down Jumpshot.

13. ~~However,~~ Gen Digital and Avast, however, continued to intercept ~~and~~, collect, store, use, and share user data through AOSP without providing adequate disclosure to users of their data theft (including the interception, collection, storage, use, and sharing of highly sensitive

Formatted: Left

Formatted: Left

Formatted: _Pld Footer Adjustment

PHI). As explained below, Gen Digital and Avast did not need to intercept, collect, store, use, or share their users' Internet search engine keyword searches, search results, ~~and~~ email inbox searches ~~through AOSP and SafePrice without providing adequate disclosure of its data theft to users.~~, browsing histories, video viewing histories, and PHI in order to provide the services promised by AOSP.

14. Gen Digital and Avast's users never consented to having Gen Digital and Avast intercept ~~and~~, collect, store, use, and share their Internet search engine keyword searches, search results, ~~and~~ email inbox searches~~.~~, browsing histories, video viewing histories, or PHI. Gen Digital and Avast's practice of ~~monitoring,~~ intercepting, ~~and~~ collecting, storing, using, and sharing user information without adequate notice amounts to a massive breach of privacy, and violates statutory, Constitutional, and common law privacy, data, and consumer protections. Further, Gen Digital and Avast's users could not have discovered the wrongful conduct at issue, which requires expertise in, among other things, inspecting and interpreting the underlying html code for the products. Indeed, users would have no reason to suspect that Gen Digital and Avast were surreptitiously intercepting their communications because (1) Gen Digital and Avast repeatedly and affirmatively represented to users that the purpose of AOSP was to prevent websites from engaging in that very conduct and (2) intercepting such communications is and was unnecessary to the purpose and function of AOSP.

15. Gen Digital and Avast's users never consented to the extraction and sale or provision of their ~~detailed~~ Internet search engine keyword searches, search results, email inbox searches, browsing ~~data~~histories, video viewing histories, and PHI to Gen Digital and Avast, from Gen Digital and Avast to third parties, from Avast to Jumpshot, or from Jumpshot to major retailers and marketers. Avast and Jumpshot's coordinated, undisclosed scheme to profit off Avast's users' personal information without adequate notice amounts to a massive breach of privacy, and violates California statutory larceny law, as well as other statutory, Constitutional, and common law privacy, data, and consumer protections.

THE PARTIES

16. Plaintiff Grace Lau is, and has been, an individual and resident of Alameda,

Formatted: Left

Formatted: _Pld Footer Adjustment

California.

17. Plaintiff Christopher Karwowski is, and has been, an individual and resident of Los Angeles, California.

18. Plaintiff Melody Klein is, and has been, an individual and resident of Arvada, Colorado.

19. Plaintiff Michael McBride is, and has been, an individual and resident of San Jose, California since August 2021. Prior to that, Plaintiff was a resident of Camino, California.

20. Plaintiff Aimen Halim is, and has been, an individual and resident of Chicago, Illinois.

~~18.~~21. Defendant Gen Digital is a foreign corporation authorized to do business in California.~~-~~ Gen Digital is organized under the laws of the State of Delaware and headquartered in Tempe, Arizona. ~~-~~Although Avast merged with Gen Digital (under its previous name NortonLifeLock) in 2022, Gen Digital continues to sell software under the trade name Avast. When "Gen Digital" and "Avast" ~~is~~are used in this complaint, ~~it refers~~given the relationship between the entities, these terms each refer to both Avast and its successor in interest~~,~~ Gen Digital.

~~19.~~22. Defendant Jumpshot was a Delaware Corporation, registered in California, whose principal office was located at 60 S. Market Street, San Jose, CA, 95113. Avast dissolved Jumpshot in January 2020, but it remains amenable to suit through the California Secretary of State.

JURISDICTION AND VENUE

~~20.~~23. The Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because it involves claims arising under the laws of the United States, including violations of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22. The Court has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

~~21.~~24. The Court also has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) and 1367 because: (i) this is a class action in which the matter in controversy exceeds the sum of $5,000,000, exclusive of interest and costs; (ii) there are 100 or more class members; and (iii) some members of the class are citizens and/or residents of different states than Defendants.

Formatted: Left

Formatted: Left

Formatted: _Pld Footer Adjustment

~~22.~~25. The Court has personal jurisdiction over Gen Digital and venue is proper in this District because ~~Gen Digital~~Defendants and Avast's intentional tortious conduct was directed by ~~Gen Digital~~Defendants and Avast into this District, including toward Plaintiff Lau~~.~~ and Plaintiff McBride. Gen Digital does extensive business within the United States, including within this District.

~~23.~~26. Gen Digital and Avast operate a website with substantial interactivity, on which U.S. consumers may download and purchase products, request refunds, and request help on billing and payment inquiries, among other features.

~~24.~~27. Gen Digital and Avast's press releases regarding the ~~products~~browser extension at issue in this case were directed at and issued from Redwood City, California and Emeryville, California.

~~25.~~28. Gen Digital and Avast advertise their products for sale in California.

~~26.~~29. Gen Digital and Avast sponsor the UC Irvine high-school cybersecurity curriculum program.

~~27.~~30. According to Avast's 2019 Annual Report, it "cooperate[s] closely" with California-based research institutions including Stanford, UC Berkeley and UC Irvine.

~~28.~~31. Also, according to its 2019 Annual Report, Avast leased property in Emeryville, California.~~-~~ This particular lease runs through June 2024. Gen Digital and Avast's website highlights its "major office" in Silicon Valley and includes several photos of the Emeryville office workspace.

~~29.~~32. Gen Digital and Avast continuously and deliberately exploit California residents for their own commercial gain.

~~30.~~33. The Court has personal jurisdiction over Jumpshot and venue is proper in this District because it is, or at all relevant times was, headquartered here and because Jumpshot has consented to California law within one or more of its commercial contracts.

~~31.~~34. The Court has personal jurisdiction over Gen Digital and Avast and venue is proper in this District because Jumpshot's tortious conduct was directed by Avast into this District, including toward Plaintiff Lau~~.~~ and Plaintiff McBride.

Formatted: _Pld Footer Adjustment

~~32.~~35. In accordance with 28 U.S.C. § 1391, venue is proper in this District because: (i) a substantial part of the conduct giving rise to Plaintiffs' claims occurred in and/or emanated from this District; (ii) Defendants transact business in this District; and (iii) Plaintiff Lau ~~resides~~and Plaintiff McBride reside in this District.

GENERAL ALLEGATIONS

I. Gen Digital and Avast ~~promises~~promise consumers privacy but ~~steals their Internet and email activity~~intercept, collect, store, use, and share consumers' private data without disclosing ~~the theft~~this misconduct.

~~33.~~36. AOSP is available to consumers for download from the Google Chrome Web Store and the Microsoft Edge Web Store. Gen Digital and Avast's webpage for AOSP proclaims that it helps consumers "[b]rowse with more privacy."[1]

~~34.~~37. Gen Digital and Avast claim that with AOSP, consumers can "[e]asily avoid malicious websites and phishing scams," "[b]lock online trackers and browse anonymously," "[o]ptimize your privacy settings on your favorite platforms," and "[t]ake the hassle out of website cookie permissions."[2] Gen Digital and Avast also claim that AOSP gives consumers "an extra level of real-time threat protection, every time you browse."[3]

~~35.~~38. Gen Digital and Avast tout AOSP's purported Privacy Features, stating that AOSP can "[k]eep your online activities private and anonymous" by keeping consumers' online activity hidden, blocking online "snoops," and by giving step-by-step privacy advice.[4] These privacy features include "Anti-tracking – prevent tracking on every website you visit;" and "Global Privacy Control – stop web companies from collecting and selling your personal data."[5]

~~36.~~39. Prior to November 2021, AOSP was called Avast Online Security ("AOS"). AOS offered protection from fake websites and phishing scams while browsing the Internet. Avast

[1] AVAST, *Online Security & Privacy*, https://www.avast.com/avast-online-security#mac (last ~~accessed November 28, 2022).~~ visited Oct. 11, 2023).

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

Formatted: Indent: Left: 0.25"
Formatted: Left
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font: Not Italic, Font color: Text 1
Formatted: Space After: 6 pt
Formatted: Font color: Text 1
Formatted: Font: Italic, Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font: Italic, Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: _Pld Footer Adjustment

claimed that AOS provided instant ratings for searches, warnings for phishing scams, malicious links and malware, and stopped websites from collecting data and tracking the users' browser history with cookies.

~~37.~~40. These assurances regarding AOSP/AOS were and are, in fact, completely hollow because AOSP continues to intercept, collect, and store users' Internet ~~browsing activity,~~ search engine keyword searches ~~and~~, search results~~. AOSP also intercepts, collects, and stores users'~~, email inbox searches~~. The same is true for SafePrice~~, browsing histories, video viewing histories, and PHI.

~~38. The SafePrice extension also intercepts, collects, and stores users' Internet browsing activity, search engine keyword searches, and email inbox searches.~~

~~39.~~41. From this information, Gen Digital and Avast—or any third party to which Gen Digital and Avast may provide the data—can recreate a user's entire web browsing history, in addition to reviewing all of their search queries and highly sensitive PHI.

~~40.~~42. As an example of how invasive this data collection can be, Internet and email searches by individuals can disclose such personal information as sexual preferences, political leanings, medical conditions or symptoms or illnesses (including abortion services), financial data, and much more. By intercepting, collecting, storing, using, and sharing such searches, Gen Digital and Avast ~~can collect~~amass and exploit a trove of information about the user, all while representing that they are protecting the user from such information being collected.

II. Avast has an established history of intercepting, collecting, storing, and selling its users' data to third parties without user consent.

~~41.~~43. Previously, Avast licensed data it intercepted ~~and~~, collected and stored to its subsidiary,[6] Jumpshot, which in turn sold the data to third party customers including Home Depot and Market Beyond. ~~-~~Those customers could and did use that data, either to better target their

[6] Avast acquired 100% of Jumpshot on September 24, 2013. It sold 35% of Jumpshot to Ascential on July 22, 2019. The sale to Ascential was reversed less than a year later when Avast repurchased the 35% interest. The repurchase transaction was completed on January 30, 2020.

Formatted: Left

Formatted: Indent: Left: 0.25", Keep with next, Keep lines together

Formatted: Left

Formatted: _Pld Footer Adjustment

advertising or to repackage it before reselling it to others.[7] The insight the data gave Jumpshot's customers into users' web browsing habits gave purchasers of that data such a commercial advantage that Jumpshot even sold information to investors looking for an informational advantage in the public securities markets.[8]

42.44. Avast acquired Jumpshot on September 24, 2013. It heralded the acquisition as one that would help keep consumer'sconsumers' data safe and their computers running at peak performance.[9]

43.45. At the time of the acquisition, Jumpshot's focus was on an application that purportedly made a consumer's computer run more efficiently by decluttering and removing so-called "junk files" from a user's computer.[10]

44.46. But over time, and in close coordination with its parent entity, Jumpshot expanded into the business of monetizing the consumer data that Avast intercepted, collected, and stored. To achieve that goal, Avast and Jumpshot entered into a licensing agreement pursuant to which Avast licensed to Jumpshot the consumer data it had intercepted, collected, and stored, and which it claimed to own.[11] In return, Jumpshot paid a fee to Avast for the data.

45.47. Avast knew that Jumpshot was selling the user data to third parties.

46.48. Avast failed to prohibit Jumpshot from selling that data, or to impose (or ensure Jumpshot adhered to) any meaningful limits on Jumpshot's use of the data it licensed to Jumpshot. And, at all relevant times, Avast maintained control over Jumpshot.

47.49. Avast did not disclose to its users that their data was being sold by Jumpshot.

---

[7] *See* Complaint filed inat ¶ 4, *Deals Way Ltd. v. Jumpshot Inc*., Case No. 3:20-CV-02988, (N.D. Cal. Filed April 30, 2020) ("Deals Way Compl.") ¶ 4. .").

[8] Thomas Brewster, *Are You One Of Avast's 400 Million Users? This Is Why It Collects And Sells Your Web Habits*, FORBES (Dec. 9, 2019)), https://www.forbes.com/sites/thomasbrewster/2019/12/09/are-you-one-of-avasts-400-million-users-this-is-why-it-collects-and-sells-your-web-habits/#180aee4d2bdc.

[9] *Id.*

[10] *Id.*

[11] Deals Way Compl. ¶32 (citing FebruaryFeb. 24, 2020, letter from Jumpshot CEO, Deren Banker).

Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font: Italic, Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: _Pld Footer Adjustment

Unbeknownst to Avast users, Jumpshot promised prospective corporate customers that they could use the data acquired from Avast to "jump the garden wall."[12] The "garden wall" is a term used to describe the universe of websites that Avast users access,[13] and at the time, Jumpshot claimed that it was "the only company that unlocks walled garden data."[14] In other words, while in the ordinary course a company would not have access to user activity on a competitor's website, Jumpshot was in the business of providing that data.

~~48.~~50. Jumpshot represented that, once in the walled garden, its customers would have access to "incredibly detailed clickstream data from 100 million global online shoppers and 20 million global app users."[15] Jumpshot promised advertisers that they could "track what users searched for, how they interacted with a particular brand or product, and what they bought."[16] Jumpshot encouraged business entities to "[l]ook into any category, country, or domain."[17]

~~49.~~51. This highly personal user information was so useful to Jumpshot's clients—who could use it to direct their advertising far more efficiently[18]—that Avast and Jumpshot could sell it for huge sums.

~~50.~~52. In total, Avast's licensing of data to Jumpshot yielded more than $20 million in annual revenue for Avast.[19]

~~51.~~53. Avast's data collection and monetization strategy through Jumpshot began to

---

[12] *Data Reports*, JUMPSHOT (via Wayback Machine) (Feb. 5, 2019), https://web.archive.org/web/20190205185953/https://www.jumpshot.com/proof_category/data-report~~/~~/.

[13] *See generally* Andrew Froehlich, *What is a walled garden on the internet?*, TECHTARGET (last updated Nov. 2021~~)~~), https://searchsecurity.techtarget.com/definition/walled-garden.

[14] *Jumpshot Strikes Strategic Partnership Deal with Ascential to Provide Marketers with Deeper Visibility into the Entire Online Customer Journey*, PRNEWSWIRE (July 22, 2019~~)~~), http://www.prnewswire.com/news-releases/jumpshot-strikes-strategic-partnership-deal-with-ascential-to-provide-marketers-with-deeper-visibility-into-the-entire-online-customer-journey-300888439.html?tc=eml_cleartime.

[15] Brewster, *supra* note ~~9~~8.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font: Italic, Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: _Pld Footer Adjustment

unravel in late 2019. On October 28, 2019, Wladimir Palant, a cybersecurity journalist, published a report detailing the personal information Avast intercepted and collected from its users. This included: (1) every website visited, alongside a user ID;[20] (2) how the user got to the page, such as by clicking on a link, or typing the address manually;[21] (3) the user's country code;[22] (4) the user's unique ID;[23] (5) what type of browser was used;[24] and, (6) in the case of the Avast antivirus product, the user's operating system and exact version number.[25]

~~52.~~54. Palant concluded that the mosaic of intercepted and collected information could be used by Avast to answer the following questions:

a. "how many tabs do you have open"?[26]

b. "what websites do you visit and when, how much time do you spend reading/watching the contents"?[27] and

c. "what do you click there and when do you switch to another tab"?[28]

~~53.~~55. Palant further concluded that users who log into their social media accounts can be deanonymized with high precision.[29] Put differently, whoever obtains the data that Avast intercepts, collects, and stores can cross reference a consumer's browsing history with a user's social media account and thus easily determine who the user is and what they are viewing online—down to each click of the mouse.

---

[20] Michael Kan, *The Cost of Avast's Free Antivirus: Companies Can Spy on Your Clicks*, PCMAG (Jan. 27, 2020), https://www.pcmag.com/news/the-cost-of-avasts-free-antivirus-companies-can-spy-on-your-clicks.

[21] Wladimir Palant, *Avast Online Security and Avast Secure Browser are spying on you*, ALMOST SECURE (Oct. 28, 2019)), https://palant.info/2019/10/28/avast-online-security-and-avast-secure-browser-are-spying-on-you/.

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

Formatted: Font color: Text 1

Formatted: _Pld Footer Adjustment

~~54.~~56. A little over a month after Palant's revelation, Mozilla—the maker of the popular web browser Firefox—learned of Avast's practices and, less then twenty-four hours later, removed four Avast security extensions.[30]

~~55.~~57. On January 27, 2020, *Vice* published an investigative piece titled *Leaked Documents Expose the Secretive Market for Your Web Browsing Data*, reporting that, "[a]n Avast antivirus subsidiary sells 'Every search. ~~-~~Every click. ~~-~~Every buy.~~-~~ On every site.'"[31] The article claimed that its findings are supported by leaked Avast documents, including contracts, internal product handbooks, and leaked consumer data.[32]

~~56.~~58. Some of that leaked consumer data revealed that Avast was selling information about consumers' personal web browsing history. ~~-~~That browsing history included information such as which pornographic sites a user visited, how long that user stayed there, and what type of pornography that user searched for. And, because the purchaser of such information was able to deanonymize the user, it was even possible for the data buyer to determine whether, for instance, an Avast user had a different sexual preference than what he or she has disclosed to the public (i.e., whether someone was gay or straight, whether out or closeted).[33]

~~57.~~59. The leaked data also showed that Avast was intercepting, collecting, and storing search queries of specific locations, including GPS coordinates on Google maps.[34] In essence, Avast was intercepting, collecting, and storing information about the precise location of where a consumer would be visiting.

~~58.~~60. The *Vice* piece further explained that after Avast intercepted, collected, and stored a consumer's data and licensed it to Jumpshot, Jumpshot sliced, repackaged and sold the data, at

---

[30] Catalin Cimpanu, *Mozilla removes Avast and AVG extensions from add-on portal over snooping claims*, (Dec. 3, 2019~~)~~), https://www.zdnet.com/article/mozilla-removes-avast-and-avg-extensions-from-add-on-portal-over-snooping-claims/.

[31] Joseph Cox, *Leaked Documents Expose the Secretive Market for Your Web Browsing Data*, VICE (Jan. 27, 2020~~)~~), https://www.vice.com/en_us/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation.

[32] *Id.*

[33] *Id.*

[34] *Id.*

Formatted: Font color: Text 1

Formatted: Font color: Text 1

Formatted: _Pld Footer Adjustment

times receiving millions of dollars for revealing consumers' "all clicks feed."[35] The Avast source reportedly described the data as being "very granular, and [] great data for these companies, because it's down to the device level with a timestamp."[36] It was also revealed that over 100 million devices had been impacted by Avast's data collection scheme.[37] As of August 2019, Jumpshot advertised having access to "100 million panelists in 188 countries."[38]

~~59.~~61. In short, while Avast was promising its users that its data would be safe and secure from data harvesters, it was harvesting such highly granular and specific information that Jumpshot advertised to its customers, without exaggeration, as offering the "most precise way to unlock human behavior online."[39]

~~60.~~62. Once Avast's business partners learned of Avast's data interception, collection and disclosure scheme, they quickly severed ties with Avast. For example, shortly after Palant's analysis was published, but before the *Vice* revelations, three major technology companies parted ways with Avast. As noted above, Mozilla discontinued its use of the Avast browser extension on December 3, 2019.[40] Technology firm Opera did the same within 16 hours of learning of Palant's analysis.[41] Roughly two weeks later, on December 18, 2019, Google removed three different Avast browser extensions from the Chrome Web Store.[42]

~~61.~~63. The reason other technology companies quickly pulled the plug on Avast is clear:

---

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] ~~Available on web archive service, the~~JUMPSHOT, https://www.jumpshot.com, (via Wayback Machine~~, available at:~~) (July 16, 2019) https://web.archive.org/web/20190716080831/https://www.jumpshot.com~~/~~/.

[39] ~~Available on web archive service, the~~JUMPSHOT, *Campaign Optimization*, (via Wayback Machine~~, available at:~~) (Feb. 15, 2019), https://web.archive.org/web/20190205175940/https://www.jumpshot.com/campaign-optimization~~/~~/.

[40] Cimpanu, *supra* note 30.

[41] Wladimir Palant, *Mozilla and Opera remove Avast extensions from their add-on stores, what will Google do?*, ALMOST SECURE (Dec. 3, 2019), https://palant.info/2019/12/03/mozilla-removes-avast-extensions-from-their-add-on-store-what-will-google-do/.

[42] Cimpanu, *supra* note 30.

Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: Font color: Text 1
Formatted: _Pld Footer Adjustment

selling such private data without users' consent is a highly intrusive invasion of privacy. The media articles highlighted the severity of Avast's intrusion upon its 400 million customers and the other technology companies did not want to be tarred with Avast's betrayal of its users' trust, much less its violations of the law.

~~62.~~64. Though Avast has claimed that the data it intercepts, collects, and stores "is fully de-identified and aggregated and cannot be used to personally identify or target" a particular user, multiple studies have shown that it is impossible to truly "anonymize" data.

~~63.~~65. A 2017 study found that web browsing histories can be linked to social media profiles using only publicly available data.[43] After developing a model for web browsing behavior, researchers were able to correctly identify 70% of users based on their web browsing histories.

~~64.~~66. By 2019, another group of researchers had developed a model that correctly identified 99.98% of Americans in any dataset using 15 demographic attributes.[44] The researchers concluded that the study's results "seriously challenge the technical and legal adequacy of the de-identification release-and-forget model."[45]

~~65.~~67. The combination of widespread and well-founded media criticism of Avast, coupled with the product distancing by market participants, pressured Avast into damage control mode. On January 30, 2020, Avast admitted (some but not all of) its improper practices and apologized.[46]

~~66.~~68. Avast also announced its plan to cease the provision of its users' data to Jumpshot and wind down Jumpshot's operations.[47]

~~67.~~69. In response to Avast's announcement that it would wind down Jumpshot, Senator

---

[43] Jessica Su ET AL., *De-anonymizing Web Browsing Data with Social Networks*, (2017) https://www.cs.princeton.edu/~arvindn/publications/browsing-history-deanonymization.pdf.

[44] Luc Rocher ET AL., *Estimating the success of re-identifications in incomplete datasets using generative models*, (July 23, 2019), https://www.nature.com/articles/s41467-019-10933-3.

[45] *Id.*

[46] Avast, *A message from Avast's CEO*, (Jan. 30, 2020~~)~~), https://blog.avast.com/a-message-from-ceo.

[47] Press Release, Avast, *Avast to Commence Wind Down of Subsidiary Jumpshot*, (Jan. 30, 2020~~)~~), https://press.avast.com/avast-to-commence-wind-down-of-subsidiary-jumpshot.

Formatted: Font color: Text 1

Formatted: Font color: Text 1

Formatted: _Pld Footer Adjustment

Ron Wyden noted that while "it is encouraging that Avast has ended some of its most troubling practices after engaging constructively with my office," he was still "concerned that Avast has not yet committed to deleting user data that was collected and shared without the opt-in consent of its users, or to end the sale of sensitive internet browsing data."[48]

~~III. Avast continues to steal its users' personal web browsing information.~~

III. Gen Digital and Avast continue to intercept, collect, store, use, and share their users' private data through AOSP, in a manner that is unnecessary for and contrary to the extension's stated purpose.

~~68.~~70. Although Avast shuttered Jumpshot after its misuse of user data was exposed in late 2019 and early 2020, Gen Digital and Avast continue to intercept ~~and~~, collect, store, use, and share users' Internet ~~and email~~ search ~~and~~engine keyword searches, search results, email inbox searches, browsing ~~activities,~~histories, video viewing histories, and PHI without providing adequate notice.

~~69.~~71. Here is how it works: ~~The Avast software~~AOSP is designed to intercept all communications from a main channel (the web browser) between the user and the websites the user visits, and copy those communications to an Avast server. ~~-~~This includes full-string, detailed URLs from the browser and full search queries, which allow Avast to track "every click, every search, and every website that [their] users visit."

~~70.~~72. For example, when a user ~~runs~~navigates to a ~~search~~webpage on ~~Google's search engine~~their Google Chrome browser, a main channel is established between the user and Google to transmit ~~communications such as search queries.~~ the URL of the webpage. The main channel communications are intercepted by AOSP (or AOS) and a copy of the communication is immediately transmitted to Gen Digital and Avast servers, and Gen Digital and Avast store the intercepted data.

73. Similarly, when a user runs a search on Google's search engine, a main channel is established between the user and Google to transmit communications such as search queries. The main channel communications are intercepted by AOSP (or AOS) and a copy of the

[48] ~~Cox, *supra* note 31.~~ Cox, *supra* note 31.

Formatted: Left

Formatted: Font color: Text 1

Formatted: _Pld Footer Adjustment

communication is immediately transmitted to Gen Digital and Avast servers, and Gen Digital and Avast store the intercepted data.

~~71.~~74. Similarly, when a user runs a search within their Gmail or Yahoo! email inbox, a main channel is created between the email user and Google or Yahoo and any search conducted by the email user is immediately intercepted by AOSP (or AOS). A copy of the search is immediately transmitted to Gen Digital and Avast servers, and Gen Digital and Avast store the intercepted data.

~~72. The SafePrice extension also captures Internet searches and searches within users' email inboxes.~~

75. ~~In light of the very names~~Defendants purposefully designed and operate AOSP to intercept, collect, and store full browser and search histories. This includes sensitive and confidential information on private areas of websites, such as medical records and banking records. AOSP was designed to intercept, collect, and store "every click, every search, and every website" in this manner despite the fact that such surreptitious mass-collection is unnecessary for its stated functions as a browser security extension: to protect privacy, defend against online threats, and prevent tracking.

76. In stark contrast to AOSP, other browser security extensions perform the same functions without persistent interception, collection, and storage of full-string URLs. For example, Norton Safe Search Enhanced ("Norton"), another popular browser security extension, operates through a local "blacklist" system that does not track users' activity in real time unless absolutely necessary. When Norton is installed, it downloads a "blacklist" of malicious websites onto the user's computer. Whenever a Norton user navigates to a particular website, that website is checked against the blacklist. Because the blacklist is locally stored, Norton does not need to track the users' activity, or communicate with any external server at all.

77. In some instances where a website does not appear on the local blacklist, Norton does send some information about the users' activity to an external server in order to perform an additional check. However, the Norton software takes two precautions to ensure that no more information is taken from the user than absolutely necessary: precautions that are notably absent from AOSP. First, Norton transmits only the domain name of the website the user visited, unlike

Formatted: Left

Formatted: _Pld Footer Adjustment

AOSP, which intercepts, collects, and stores the full-string URL. Second, once Norton identifies that the website is ***not*** malicious, it ceases collection of all browsing history—including domain names—for that website.

78. For example, if a user were to visit "https://www.hhs.gov/hipaa/for-professionals/privacy/index.html," Norton would collect only "www.hhs.gov" and use that domain name to determine whether hhs.gov was a safe website. Once this is confirmed, Norton would not track any other browsing or searching from the same user on hhs.gov. AOSP, in contrast, would intercept, collect, and store the entire URL, and continue to do so for every single page the user visited on hhs.gov, even after it determines that hhs.gov is a safe website.

79. Not only is Norton's local blacklist method equally effective at ensuring security, it also does so more efficiently than AOSP's persistent interception, collection, and storage method. Unlike Norton, which can check most websites locally without communicating with an external server, AOSP requires constant communication between the user's device and AOSP's server, creating a significant resource drain on both ends. Not only does this make web browsing slower for the user, it is also much more expensive to operate for Defendants—because it requires significantly more computing power.

80. Gen Digital chooses the higher cost of using the persistent interception, collection, and storage method instead of the local blacklist method, because it profits from the private data intercepted, collected, and stored by AOSP. To this end, AOSP uses approximately ***forty-five*** third-party advertising cookies designed to transmit the intercepted, collected, and stored data on its servers to numerous third-party advertising partners, including Google, MS Advertising, and Adalyser. Through these cookies, private data intercepted, collected, and stored by AOSP—including the data discussed below—was and is provided for use by these third parties for targeted advertising, to the financial benefit of Defendants.

81. These third-party advertising cookies are unnecessary for browser security purposes. They are tacked onto AOSP in order to monetize more private data. No such third-party advertising cookies exist on Norton.

82. Further, Defendants employ deceptive practices in order to conceal from users that

Formatted: _Pld Footer Adjustment

these third-party advertising cookies are being installed on their computer through AOSP. For example, AOSP guides its users to a cookie banner asking whether they wish to accept all cookies, or only "strictly necessary" cookies. However, ***regardless of the option chosen, approximately the same number of cookies are installed***. On information and belief, Defendants created this deceptive cookie banner in order to lull users into a false sense of security, and trick them into thinking that they could block third-party advertising cookies by choosing the "strictly necessary" option.

83. Critically, Defendants cannot claim ignorance of how Norton and other security extensions like it operate, because ***Norton is also owned and operated by Defendant Gen Digital***. Defendants know full well how to design and operate a browser security extension without persistent interception, collection, and storage of full-string detailed URLs. They have simply chosen not to do so with regards to AOSP because they profit handsomely from the interception, collection, and storage of private data.

~~73.~~84. In light of the very name of the Avast Online Security & Privacy ~~and SafePrice products, as well as~~extension, Gen Digital and Avast's repeated representations highlighted above regarding how ~~these products~~that extension purportedly protect users' personal information, ~~consumers~~ as well as the fact that persistent interception, collection, and storage of full-string detailed URLs and use of third-party advertising cookies are completely unnecessary for the function of a browser security extensions, AOSP users are led to believe that their private ~~Internet and email searches and browsing activity are safe~~data is safe. The fact that AOSP is in fact eavesdropping on the contents of their search and browsing histories, and is duplicating and communicating such histories to Defendants, is completely unknown to users.

IV. The private data stolen by Gen Digital and Avast includes highly sensitive and personally-identifiable PHI from Kaiser Permanente members.

85. Patient health care information in the United States is protected by federal law under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and HIPAA's implementing regulations promulgated by the United States Department of Health and Human Services ("HHS"). The "HIPAA Privacy Rule," (45 CFR Part 160 and Subparts A and E of Part

Formatted: Left

Formatted: _Pld Footer Adjustment

164)[49] establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as "protected health information" or "PHI"). The HIPAA Privacy Rule applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The HIPAA Privacy Rule requires such entities to implement appropriate safeguards to protect the privacy of PHI. It also sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization. The HIPAA Privacy Rule also gives individuals rights over their PHI, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their PHI in an electronic health record, and to request corrections.

86. The HIPAA Privacy Rule defines PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

87. Non-party Kaiser Permanente ("Kaiser") is an integrated managed care consortium of for-profit and non-profit entities, headquartered in Oakland, California. It operates 39 hospitals across eight states (California, Washington, Oregon, Colorado, Hawaii, Georgia, Maryland, and Virginia).[50] Kaiser serves a total of 12.6 million members, and approximately 9.4 million of them (or roughly 75%) reside in California.

88. Kaiser operates a website at https://healthy.kaiserpermanente.org/ (the "Kaiser Website") through which it communicates with its members ("Kaiser Members") and non-members. By logging into their individual patient portal ("Kaiser Account"), Kaiser Members can make appointments, search for doctors, review and manage their prescriptions, and review their medical records and medical history.

89. Whenever a user with AOSP installed on their device navigates the Kaiser Website,

[49] *See* U.S. Dep't of Health & Hum. Servs, *Summary of the HIPAA Privacy Rule,* (last reviewed Oct. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[50] *See* KAISER PERMANENTE, *Who we are: Fast Facts*, https://about.kaiserpermanente.org/who-we-are/fast-facts (last visited Oct. 11, 2023).

Formatted: _Pld Footer Adjustment

AOSP intercepts and collects every single click and search query, and it transmits the URL of every webpage visited to Gen Digital and Avast's servers. This happens regardless of whether or not the user is a Kaiser Member, is logged into a Kaiser Account, or is in a protected area of the Kaiser Website. With respect to Kaiser Members who are logged into their Kaiser Accounts, the intercepted, collected, and stored URLs and webpage titles divulge to Gen Digital and Avast some or all of the Kaiser Members' medical history and PHI, including the medications the Kaiser Member is prescribed, the medical conditions the Kaiser Member suffers from, the Kaiser Member's immunization record, and the Kaiser Member's allergies.

90. When logged in to their Kaiser Account on the Kaiser Website, Kaiser Members can view each of their medical conditions by navigating to a personalized "Medical Record" page and then further navigating to a personalized "Health Summary" page. When viewing their list of medical conditions, for example, each listed condition contains a hyperlink reading "Learn more," which, when clicked, automatically runs a search on the Kaiser Website for that medical condition. The search uses the name of the condition as a search query and navigates the Kaiser Member to a webpage on the Kaiser Website containing the search results. The URL for that webpage also contains the name of the condition.

91. Unbeknownst to Kaiser Members, when a Kaiser Member clicks on the "Learn more" hyperlink for a given medical condition, AOSP intercepts, collects, and stores the URL of the page containing the search results, which contains the name of the medical condition used for the search query and reveals that the Kaiser Member navigated to the page containing the search results from the Kaiser Member's personalized "Medical Record" page accessed from the Kaiser Member's Kaiser Account.

92. From the personalized "Health Summary" page, a Kaiser Member can view their immunization history by selecting the "Immunizations" tab. Each listed immunization contains a hyperlink reading "Learn more," which, when clicked, automatically runs a search on the Kaiser Website for the immunization using the name of the immunization as a search query. The Kaiser Website navigates the Kaiser Member to a webpage on the Kaiser Website containing the search results. Unbeknownst to Kaiser Members, when a Kaiser Member clicks on the "Learn more"

Formatted: _Pld Footer Adjustment

hyperlink for a given immunization, AOSP intercepts, collects, and stores the URL of the page containing the search results, which contains the name of the immunization used for the search query and reveals that the Kaiser Member navigated to the page containing the search results from the Kaiser Member's personalized "Medical Record" page accessed from the Kaiser Member's Kaiser Account.

93. Also from the personalized "Health Summary" page, a Kaiser Member can view a list of their allergies by selecting the "Allergies" tab. When viewing their list of allergies, each listed allergy contains a hyperlink reading "Learn more," which, when clicked, automatically runs a search on the Kaiser Website for the allergy using the name of the allergy as a search query. The website navigates the Kaiser Member to a webpage on the Kaiser Website containing the search results. Unbeknownst to Kaiser Members, when a Kaiser Member clicks on the "Learn more" hyperlink for a given allergy, AOSP intercepts, collects, and stores the URL of the page containing the search results, which contains the name of the allergy used for the search query and reveals that the Kaiser Member navigated to the page containing the search results from the Kaiser Member's personalized "Medical Record" page accessed from the Kaiser Member's Kaiser Account.

94. Because the intercepted, collected, and stored data shows that the Kaiser Member accessed the relevant pages from the Kaiser Member's "Medical Records" page, which is only accessible while logged in, Gen Digital is aware that the individual is a Kaiser Member.

95. In addition, when logged into their Kaiser Account through the Kaiser Website, Kaiser Members can view each of their prescribed medications by navigating to their personalized "Prescription Details" page. When viewing the list of medications, Kaiser Members are able to click on a medication to navigate to a webpage within Kaiser's "Drug encyclopedia" with additional information about that medication in order to learn more about it. Unbeknownst to Kaiser Members, when a Kaiser Member clicks on a medication and navigates to that medication's "Drug encyclopedia" webpage, AOSP intercepts, collects, and stores the URL for that page, which includes the medication's reference number in Kaiser's "Drug encyclopedia," which specifically identifies the drug and transmits the name of the medication.

Formatted: _Pld Footer Adjustment

96. The above-described data is PHI, since it is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

97. AOSP utilizes third-party cookies to transmit the intercepted, collected, and stored data to third-party advertising partners including Google, MS Advertising, and Adalyser, to the financial benefit of Gen Digital and Avast. For example, the third-party cookie from Adalyser, an advertising platform, is titled "__adal_id" (the "Adalyser Cookie"). The Adalyser Cookie stores a unique identifier known as a "Device ID" for each device that accesses a website.[51] The Adalyser Cookie is a "persistent" cookie, which remains constant across different sessions from the same device, thus allowing websites to "remember" users across multiple visits.

98. AOSP also intercepts, collects, and stores the unique Device ID generated by the Adalyser Cookie. This identifier allows Gen Digital and Avast to link the private data—including but not limited to PHI—intercepted and collected from Kaiser Website users' and Kaiser Members' communications with the Kaiser Website—including but not limited to the above communications concerning medications, medical conditions, immunizations, and allergies—across multiple sessions to the specific Kaiser Website user.

99. Kaiser Website users, including Kaiser Members accessing their Kaiser Accounts, are unaware and have no way of knowing that Gen Digital and Avast are intercepting, collecting, and storing the above-described data through AOSP, and have not provided their consent, whether implied or express, for AOSP to intercept, collect or store this data.

V. The private data stolen by Gen Digital and Avast includes sensitive video viewing information from Hulu.

100. Non-party Hulu is a popular subscription streaming video website that is majority-owned and operated by the Walt Disney Company. As of January 1, 2023, Hulu has an estimated 48 million subscribers in the U.S. and Canada.[52] Hulu operates a website at https://www.hulu.com/

[51] *Adalyser cookies*, https://www.adalyser.com/en/cookies (last visited Oct. 11, 2023) (describing the purpose of this cookie as "[u]niquely identify[ing] a device, [and] stor[ing] a generated Device ID.").

[52] *Id.*

Formatted: _Pld Footer Adjustment

(the "Hulu Website"), from which users can browse and view or stream video content, including television programs and movies.

101. Whenever a user with AOSP installed on their device navigates the Hulu Website, AOSP intercepts, collects, and stores every single click and search query, and transmits the URL of every webpage visited to Gen Digital and Avast's servers. This happens regardless of whether or not the user is logged into Hulu. The intercepted, collected, and stored URLs and webpage titles divulge to Gen Digital and Avast the names of the videos that the user has browsed or watched.

102. The third-party cookies (listed above) allow Gen Digital and Avast to transmit the data to those third parties, and to link the private data intercepted and collected from the Hulu Website across multiple sessions to the specific user, thus identifying every video that a particular user has browsed or watched—tying that video to that particular user.

103. Hulu Website users are unaware and have no way of knowing that Gen Digital and Avast are intercepting, collecting and storing the above-described data through AOSP, and have not provided their consent, whether implied or express, for AOSP to intercept, collect or store this data.

VI. The private data stolen by Gen Digital and Avast has economic value, and there is a market for such private data.

104. The value of private data is well understood and generally accepted as a form of currency. It is by now incontrovertible that a robust market for this data undergirds the tech economy.

105. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[53] A 2015 article from TechCrunch accurately noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."[54] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more

[53] *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[54] Pauline Glikman & Nicolas Glady, *What's The Value Of Your Data?*, TECHCRUNCH (Oct. 13, 2015), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/.

Formatted: _Pld Footer Adjustment

than $40.[55]

106. Recent years have witnessed a notable transition in private data collection methodologies. The traditional avenues, such as surveys, have experienced a decline as more advanced and automated techniques gain traction.[56] The shift was propelled by market conditions that necessitate novel approaches to engage individuals, culminating in a diminished reliance on surveys and an uptick in real-time consumer data harvesting through various online platforms.[57]

107. The Organization for Economic Cooperation and Development ("OECD") itself has published numerous volumes discussing how to value data such as that which is the subject matter of this Complaint, including as early as 2013, with its publication "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value".[58] The OECD recognizes that data is a key competitive input not only in the digital economy but in all markets: "Big data now represents a core economic asset that can create significant competitive advantage for firms and drive innovation and growth."[59]

108. In *The Age of Surveillance Capitalism*, Harvard Business School Professor Shoshanna Zuboff notes that large corporations like Verizon, AT&T and Comcast have transformed their business models from fee for services provided to customers to monetizing their user's data—including user data that is not necessary for product or service use, which she refers to as "behavioral surplus."[60] In essence, Professor Zuboff explains that revenue from Internet user

---

[55] *Id.*

[56] *See generally* Lorena Blasco-Arcas ET AL., *The Role of Consumer Data in Marketing: A Research Agenda*, 146 J. BUS. RES. 436, 436-452 (2022).

[57] *Id.*

[58] OECD, Exploring the Economics of Personal Data, OECD PUBLISHING (Apr. 2, 2013), http://dx.doi.org/10.1787/5k486qtxldmq-en.

[59] OECD, *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD PUBLISHING (Oct. 10, 2013) https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledge-capital-growth-and-innovation_9789264193307-en.

[60] Shoshanna Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 166 (2019).

Formatted: _Pld Footer Adjustment

data pervades every economic transaction in the modern economy. It is a fundamental assumption of these revenues that there is a *market* for this data; data generated by Internet users using AOSP has economic value.

109. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: "Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."[61]

110. The awareness among consumers regarding the value of their personal data has seen a significant upswing. Nearly one-third of all consumers would not sell their personal private data for any amount of money.[62] Historically, individuals were often remunerated for their participation in surveys with monetary rewards.[63] Now, they recognize that the personal information they furnish to companies holds value and furnishes actionable insights, enabling firms to sculpt effective business strategies.[64]

111. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. The data, however, also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiffs herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet

[61] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

[62] Adswerve, *Consumers Price Out the Value of Personal Data*, ADSWERVE (June 15, 2021) https://adswerve.com/blog/consumers-price-out-the-value-of-personal-data/.

[63] SurveyMonkey, *Survey Prizes: Pros and Cons, SurveyMonkey*, https://www.surveymonkey.com/mp/survey-prizes-pros-and-cons/ (last visited Oct. 5, 2023).

[64] Roger Horberry, *Why Your Market Research Team is More Valuable Than Ever*, GLOBALWEBINDEX (February 3, 2021), https://blog.gwi.com/marketing/market-research-more-valuable-than-ever/ (last visited Oct. 5, 2023).

Formatted: _Pld Footer Adjustment

users for their data.[65] Likewise, apps such as Zynn pay users to sign up and interact with the app.[66]

112. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

113. As Professors Acquisti, Taylor, and Wagman relayed in their 2016 article "The Economics of Privacy," published in the *Journal of Economic Literature*,

> [s]uch vast amounts of collected data have obvious and substantial economic value. Individuals' traits and attributes (such as a person's age, address, gender, income, preferences, and reservation prices, but also her clickthroughs, comments posted online, photos uploaded to social media, and so forth) are increasingly regarded as business assets that can be used to target services or offers, provide relevant advertising, or be traded with other parties.[67]

114. There is also a private market for Internet users' personal information. While there is a wide range in values, the prices are nonetheless significant. For example:

> Each piece of personal info has a price tag. A Social Security number may sell for as little as $1. Credit card, debit card and banking info can go for as much as $110. Usernames and passwords for non-financial institution logins are $1, but it can range from $20 to $200 for login info for online payment platforms.[68]
>
> Researchers pored through the prices of personal data and information—called 'fullz' by those searching for 'full credentials'—that are available for sale on nearly 50 different Dark Web marketplaces, finding that Japan, the UAE, and EU countries have the most expensive identities available at an average price of $25.[69]

---

[65] Kevin Mercadante, *10 Apps for Selling Your Data for Cash*, BEST WALLET HACKS (July 17, 2023), https://wallethacks.com/apps-for-selling-your-data/.

[66] Jacob Kastrenakes, *A new TikTok clone hit the top of the App Store by paying users to watch videos*, THE VERGE (May 29, 2020), https://www.theverge.com/2020/5/29/21274994/zynn-tiktok-clone-pay-watch-videos-kuaishou-bytedance-rival.

[67] Alessandro Acquisti ET AL., *The Economics of Privacy*, 54 J. OF ECON. LITERATURE 2, at 444 (June 2016), https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf.

[68] Understanding the Illegal Market for Personal Information, ONPOINT, https://www.onpointcu.com/blog/understanding-the-illegal-market-for-personal-information/#:~:text=Each%20piece%20of%20personal%20info,info%20for%20online%20payment%20platforms (last visited Oct. 11, 2023).

[69] Jonathan Greig, *How much is your info worth on the Dark Web? For Americans, it's just $8,*

Formatted: _Pld Footer Adjustment

> According to Comparitech, who researched the prices of stolen credit cards, hacked PayPal accounts, and private Social Security numbers on more than 40 different dark web marketplaces, the average price of each U.S. citizen's "fullz," or complete information including name, date of birth, address, phone number, account numbers and other information is $8.[70]

115. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

116. Moreover, a stark contrast exists between the modus operandi of data collection today as compared to the past. Unlike surveys, contemporary data harvesting often occurs without explicit consent and devoid of any compensatory offer to the consumer. This method proves to be a more lucrative and higher return on investment for entities as opposed to the earlier practice of crafting surveys, disseminating them, and compensating the respondents.[71]

117. Avast profits from this covert data harvesting practice to the detriment of the Class and Subclass members. The market for personal data exists and is thriving, but individual consumers like the Class and Subclass members have fewer opportunities to market their data for value, thereby diminishing the value of their data to them, when companies like Avast are already secretly harvesting and selling the same data to third parties themselves.

118. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

TECHREPUBLIC (Feb. 8, 2021), https://www.techrepublic.com/article/how-much-is-your-info-worth-on-the-dark-web-for-americans-its-just-8/.

[70] *There's Value in Everything: Stop Underestimating the Value of Your Data on the Black Market*, VIRTUALLY MANAGED IT SOLUTIONS, https://vmits.com/theres-value-in-everything-stop-underestimating-the-value-of-your-data-on-the-black-market/ (last visited Oct. 11, 2023).

[71] *See generally* Michael McFarland, SJ, *Unauthorized Transmission and Use of Personal Data*, MARKKULA CENTER FOR APPLIED ETHICS AT SANTA CLARA UNIVERSITY, SCU, https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/unauthorized-transmission-and-use-of-personal-data/ (last visited Oct. 5, 2023).

Formatted: _Pld Footer Adjustment

VII. Plaintiffs and Class and Subclass members suffered an economic injury.

119. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things such as data or communications.

120. California courts have recognized the lost "property value" of personal information. Recent changes in California law have also confirmed that individuals have a property interest in their information. In 2018, California enacted the California Consumer Privacy Act ("CCPA"). Among other things, the CCPA permits businesses to purchase consumer information from consumers themselves (Cal. Civ. Code § 1798.125(b)(1)) and permits businesses to assess and appraise – *i.e.*, to place a monetary value on – consumer data (Cal. Civ. Code § 1798.125(a)(2)).

121. Accordingly, Plaintiffs' and Class and Subclass members' private data is property under California law.

122. Defendants' interception, collection, storage, use, and sharing of Plaintiffs' and Class and Subclass members' private data without authorization is a taking of Plaintiffs' and Class and Subclass members' property. Plaintiffs and Class and Subclass members have a right to disgorgement and/or restitution damages for the value of the improperly intercepted and collected private data by Defendants through AOSP.

123. Plaintiffs and Class and Subclass members have suffered benefit of the bargain damages, in that Defendants took more data than authorized. Those benefit of the bargain damages also include, but are not limited to (i) loss of the promised benefits of their use of AOSP; (ii) out-of-pocket costs; and (iii) loss of control over property which has marketable value.

124. To preserve their privacy, Plaintiffs and Class and Subclass members who now understand at least some of Defendants' violations are presented with the choice of (i) discontinuing use of AOSP; or (ii) knowingly accepting less privacy than they were promised. Each of these options deprives Plaintiffs and Class and Subclass members of the benefits of their original bargain. There is no option that recovers the property improperly intercepted and collected by Defendants.

125. Further, Plaintiffs and Class and Subclass members were denied the benefit of knowing that Defendants were intercepting, collecting, storing, using, and sharing their private

Formatted: _Pld Footer Adjustment

data. Thus, they were unable to mitigate the harms they incurred because of Defendants' actions. That is, Defendants' lack of transparency prevented and still prevents Plaintiffs' and Class and Subclass members' ability to mitigate the harms.

126. Defendants avoided costs they should have incurred because of their actions. If they disclosed their actions, they would have suffered losses as users would have been discouraged from using AOSP.

127. Defendants thus were not only able to evade or defer these costs, but they were able to continue to accrue value and further benefit from the delay due to the time value of money. Defendants have thus transferred all of the costs imposed by the unauthorized interception and collection of users' private data onto Plaintiffs and Class and Subclass members. Defendants increased the cost to Plaintiffs and Class and Subclass members of mitigating the interception and collection of their private data by failing to notify them that Defendants were intercepting, collecting, storing, using, and sharing Plaintiffs' and Class and Subclass members' private data.

128. In addition, Plaintiffs and Class and Subclass members have suffered from the diminished value of their own private data, which is property that has both personal and economic value to Plaintiffs and Class and Subclass members.

129. Plaintiffs' and Class and Subclass members' private data have different forms of value. First, there is transactional, or barter, value. Indeed, Defendants could have offered that consumers could use AOSP in return for allowing Defendants to intercept, collect, store, use, and share their personal data, including PHI. Defendants did not, but instead chose to conceal the extent to which they intercepted, collected, stored, used, and shared consumers' information.

130. Second, Plaintiffs' and Class and Subclass members' property, which has economic value, was taken from them without their consent. There is a market for this private data, and it has at minimum a value greater than zero. Plaintiffs and Class and Subclass members cannot bring their private data to market because Defendants already have intercepted, collected, stored, used, and shared that private data for particular advertising purposes. Data purchasers, therefore, have no need to acquire the data from Plaintiffs and Class and Subclass members.

131. Third, in addition to the monetary value of selling their data, Plaintiffs and Class

Formatted: _Pld Footer Adjustment

and Subclass members also assign value to keeping their private data private. It is possible to quantify this privacy value, which is destroyed when Defendants intercept, collect, store, use, and share Plaintiffs' and Class and Subclass members' private data without notice or authorization.

132. Plaintiffs and Class and Subclass members were harmed when Defendants took their property and exerted exclusive control over it, intercepting, collecting, storing, using, and sharing it without Plaintiffs' and Class and Subclass members' knowledge to benefit Defendants and for still undisclosed purposes.

133. Further, Defendants' control over ever-expanding digital dossiers on users, which include the private data and PHI discussed above, makes tracking and profiling Plaintiffs and Class and Subclass members, and targeting them with advertising, much more efficient and effective. Defendants unjustly earn substantial profits from such targeted advertising and/or from the sale of user data and/or information or services derived from such data.

134. In sum, Defendants have intercepted, collected, stored, used, and shared Plaintiffs' and Class and Subclass members' private data without providing anything of value to Plaintiffs and Class and Subclass members in exchange for that private data. Moreover, Defendants' unauthorized access to Plaintiffs' and Class and Subclass members' private data has diminished the value of that private data. These actions and omissions by Defendants have resulted in harm to Plaintiffs and Class and Subclass members.

NAMED PLAINTIFF ALLEGATIONS

~~74.~~135. **Plaintiff Grace Lau** used ~~both~~ AOSP ~~and SafePrice, both~~ on the Chrome web browser~~,~~ for years, through mid-2021. ~~Ms.~~Plaintiff Lau believed that using ~~Avast Online Security & Privacy~~AOSP would help protect her privacy, and she was unaware and could not have known that ~~Avast was~~Defendants were intercepting ~~and~~, collecting, storing, using, and sharing her Internet search engine keyword searches, search results, ~~and~~ email inbox searches~~. Ms.~~, and browsing history, which Defendants did throughout the time that Plaintiff Lau ~~would not have~~ used ~~the Avast products~~AOSP. Plaintiff Lau would not have used AOSP had she known that ~~they were~~it was invading her privacy.

~~75.~~136. Plaintiff Lau has incurred harm as a result of Defendants' invasion of her

Formatted: Font: Bold
Formatted: Left

Formatted: _Pld Footer Adjustment

privacy rights through the unauthorized interception, collection, ~~and~~storage, use, and sharing of her Internet search engine keyword searches, search results, ~~and~~ email inbox searches~~.~~, and browsing history. Defendants' taking Plaintiff Lau's information lessens the value of that information to Plaintiff Lau and third parties with whom Plaintiff Lau has in the past, and would like in the future, to engage in market transactions concerning her information. In particular, Plaintiff Lau has participated in market research studies for which she has been paid, and the value of her participation is decreased due to the fact that Defendants make available extensive information about her consumer preferences and activity without paying Plaintiff Lau. Similarly, Plaintiff Lau has, at her election, exchanged her personal information for discounts via reward programs, and Defendants' taking reduces the value of Plaintiff Lau's personal information in those types of exchanges.

137. Plaintiff Lau would like to continue to use AOSP and would do so if it did not invade her privacy through the unauthorized interception, collection, storage, use, and sharing of her Internet search engine keyword searches, search results, email inbox searches, and browsing history.

138. In addition, Plaintiff Lau may begin using AOSP again in the future under the reasonable but mistaken assumption that it would no longer invade her privacy through the unauthorized interception, collection, storage, use, and sharing of her Internet search engine keyword searches, search results, email inbox searches, and browsing history.

~~76.~~139. **Plaintiff Christopher Karwowski** used ~~both~~ AOSP ~~and SafePrice~~, both on the Chrome web browser, from 2019-2020. ~~Mr.~~Plaintiff Karwowski believed that using ~~Avast Online Security & Privacy~~AOSP would help protect his privacy, and was unaware ~~that Avast was taking~~ and could not have known that Defendants were intercepting, collecting, storing, using, and sharing his Internet search engine keyword searches, search results, ~~and~~ email inbox searches~~.~~ ~~Mr.~~, and browsing history, which Defendants did throughout the time that Plaintiff Karwowski used AOSP. Plaintiff Karwowski would not have used ~~the Avast products~~AOSP had he known that ~~they were~~it was invading his privacy.

~~77.~~140. Plaintiff Karwowski has incurred harm as a result of Defendants' invasion

Formatted: Font: Bold

Formatted: Left

Formatted: _Pld Footer Adjustment

of his privacy rights through the unauthorized interception, collection, storage, use, and ~~use~~sharing of his Internet search engine keyword searches, search results, ~~and~~ email inbox searches~~.~~, and browsing history. Plaintiff Karwowski participates in the market for his personal data, including by exchanging it at his election for discounts and stores, and Defendants' taking reduces the value of Plaintiff Karwowksi's personal information in those types of exchanges

141. Plaintiff Karwowski would like to continue to use AOSP and would do so if it did not invade his privacy through the unauthorized interception, collection, storage, use, and sharing of his Internet search engine keyword searches, search results, email inbox searches, and browsing history.

142. In addition, Plaintiff Karwowski may begin using AOSP again in the future under the reasonable but mistaken assumption that it would no longer invade his privacy through the unauthorized interception, collection, storage, use, and sharing of his Internet search engine keyword searches, search results, email inbox searches, and browsing history.

143. **Plaintiff Melody Klein** used AOSP on the Chrome web browser starting in early 2023. Plaintiff Klein believed that using AOSP would help protect her privacy, and she was unaware and could not have known that Defendants were intercepting, collecting, storing, using and sharing her Internet search engine keyword searches, search results, email inbox searches, browsing history, and Kaiser Website activity (including her and her children's PHI), which Defendants did throughout the time that Plaintiff Klein used AOSP. Plaintiff Klein would not have used AOSP had she known that it was invading her privacy.

144. Plaintiff Klein, a Kaiser Member, uses the Kaiser website to manage the medical records of both herself and her children, and she has done so after installing AOSP. In particular, Plaintiff Klein has used the Kaiser Website to schedule appointments, refill prescriptions, review medical test results and immunization records, send messages to doctors, and pay medical bills. Plaintiff Klein had assumed that this information would be completely secure and private.

145. Plaintiff Klein has incurred harm as a result of Defendants' invasion of her privacy rights through the unauthorized interception, collection, storage, use, and sharing of her Internet search engine keyword searches, search results, email inbox searches, browsing history, and her

Formatted: _Pld Footer Adjustment

and her children's PHI.

146. Defendants' taking of Plaintiff Klein's information lessens the value of that information to Plaintiff Klein and third parties with whom Plaintiff Klein has in the past, and would like in the future, to engage in market transactions concerning her information. Plaintiff Klein shares her personal information with companies when adequately informed and compensated. In particular, Plaintiff Klein has participated in consumer surveys at National Hockey League games, where she is entered to win either cash or gift cards in exchange for answering questions related to her preferences and experience at the game. Plaintiff Klein also has participated in market research studies concerning consumer products such as toothbrushes and frozen foods, where she is provided with gift cards in exchange for providing information on her preferences and opinions about how these products are marketed.

147. The value of Plaintiff Klein's participation is decreased due to the fact that Defendants make available extensive information about her consumer preferences and activity without paying her.

148. Plaintiff Klein would like to continue to use AOSP and would do so if it did not invade her privacy through the unauthorized interception, collection, storage, use, and sharing of her Internet search engine keyword searches, search results, email inbox searches, browsing history, and her and her children's PHI.

149. In addition, Plaintiff Klein may begin using AOSP again in the future under the reasonable but mistaken assumption that it would no longer invade her privacy through the unauthorized interception, collection, storage, use, and sharing of her Internet search engine keyword searches, search results, email inbox searches, browsing history, and her and her children's PHI.

150. **Plaintiff Michael McBride** used AOSP on the Chrome web browser from 2019-2023. Plaintiff McBride believed that using AOSP would help protect his privacy, and was unaware and could not have known that Defendants were intercepting, collecting, storing, using, and sharing his Internet search engine keyword searches, search results, email inbox searches, browsing history, and Kaiser Website activity (including his PHI), which Defendants did

Formatted: _Pld Footer Adjustment

throughout the time that Plaintiff McBride used AOSP. Plaintiff McBride would not have used AOSP had he known that it was invading his privacy.

151. Plaintiff McBride was a Kaiser Member using the Kaiser Website to manage his medical records from 2018 to 2020. After he stopped being a Kaiser Member, Plaintiff McBride enrolled in a Kaiser-sponsored weight loss program, and continued to use the Kaiser Website to manage his account, make appointments, and participate in weekly video calls through August 2021. Plaintiff McBride had assumed that this information would be completely secure and private.

152. Plaintiff McBride has incurred harm as a result of Defendants' invasion of his privacy rights through the unauthorized interception, collection, storage, use, and sharing of his Internet search engine keyword searches, search results, email inbox searches, browsing history, and PHI (including in connection with the Kaiser-sponsored weight loss program).

153. Defendants' taking of Plaintiff McBride's information lessens the value of that information to Plaintiff McBride and third parties with whom Plaintiff McBride has in the past, and would like in the future, to engage in market transactions concerning his information. In particular, Plaintiff McBride regularly participates in consumer surveys, including Taco Bell and Walmart surveys, related to food and experiences or after purchasing a product or service for value. In return for completing the surveys, Plaintiff McBride is entered for the chance to win cash prizes. The value of Plaintiff McBride's participation is decreased due to the fact that Defendants make available extensive information about his consumer preferences and activity without paying him.

154. Plaintiff McBride would like to continue to use AOSP and would do so if it did not invade his privacy through the unauthorized interception, collection, storage, use, and sharing of his Internet search engine keyword searches, search results, email inbox searches, browsing history, and PHI.

155. In addition, Plaintiff McBride may begin using AOSP again in the future under the reasonable but mistaken assumption that it would no longer invade his privacy through the unauthorized interception, collection, storage, use, and sharing of his Internet search engine

Formatted: _Pld Footer Adjustment

keyword searches, search results, email inbox searches, browsing history, and PHI.

156. **Plaintiff Aimen Halim** used AOSP on the Chrome web browser, from 2021-2023. Plaintiff Halim believed that using AOSP would help protect his privacy, and was unaware and could not have known that Defendants were intercepting, collecting, storing, using, and sharing his Internet search engine keyword searches, search results, email inbox searches, browsing history, and Hulu Website activity (including his video viewing history), which Defendants did throughout the time that Plaintiff Halim used AOSP. Plaintiff Halim would not have used AOSP had he known that they were invading his privacy.

157. Plaintiff Halim has had a Hulu account since January 2022, and has accessed it approximately two to three times a week using the Chrome web browser on the same laptop where the AOSP extension is installed.

158. Plaintiff Halim has incurred harm as a result of Defendants' invasion of his privacy rights through the unauthorized interception, collection, storage, use and sharing of his Internet search engine keyword searches, search results, email inbox searches, browsing history, and Hulu Website activity (including his video viewing history).

159. Defendants' taking of Plaintiff Halim's information lessens the value of that information to Plaintiff Halim and third parties with whom Plaintiff Halim has in the past, and would like in the future, to engage in market transactions concerning his information. In particular, Plaintiff Halim regularly shares his personal information with companies when adequately informed and compensated. For example, he served as a TVision TV panelists for two years in return for monthly cash payments and other incentives. TVision measures TV and streaming viewership using webcams to determine, among other things, whether viewers are actually paying attention to the advertisements on their television screen. The value of Plaintiff Halim's participation is decreased due to the fact that Defendants make available extensive information about his consumer preferences and activity without paying him.

160. Plaintiff Halim would like to continue to use AOSP and would do so if it did not invade his privacy through the unauthorized interception, collection, storage, use and sharing of his Internet search engine keyword searches, search results, email inbox searches, browsing

Formatted: _Pld Footer Adjustment

history, and Hulu Website activity (including his video viewing history).

161. In addition, Plaintiff Halim may begin using AOSP again in the future under the reasonable but mistaken assumption that it would no longer invade his privacy through the unauthorized interception, collection, storage, use and sharing of his Internet search engine keyword searches, search results, email inbox searches, browsing history, and Hulu Website activity (including his video viewing history).

CHOICE OF LAW

~~78.~~162. California's substantive laws may be constitutionally applied to the Plaintiffs' and the Nationwide Class members' claims under the Due Process Clause, 14th Amend., § 1, and the Full Faith and Credit Clause, art. IV., § 1, of the U.S. Constitution.

~~79.~~163. California has a significant contact, or significant aggregation of contacts, to the claims asserted by each Plaintiff, thereby creating state interests that ensure that the choice of California state law to the common-law claims is not arbitrary or unfair. Gen Digital and Avast conducted substantial business in California, and Jumpshot was headquartered in California. California has a strong interest in regulating Gen Digital, Avast, and Jumpshot's conduct under its laws.

164. Further, Avast utilizes physical servers located in California for the operation of its AOSP software. The Kaiser Website – from which Defendants intercepted PHI – was also operated through physical servers located in California.

~~80.~~165. The application of California law to the proposed Nationwide Class members (defined below) is also appropriate under California's choice of law rules, namely, the governmental interest test California uses for choice-of-law questions. California's interest would be the most impaired if its laws were not applied.

DISCOVERY RULE, TOLLING, AND FRAUDULENT CONCEALMENT, ~~AND ESTOPPEL~~

166. ~~The~~All applicable statutes of limitation have been tolled by operation of the discovery rule, which delays accrual until plaintiff has, or should have, inquiry notice of the cause of action. First, in light of Defendants' affirmative statements (discussed above and below) and

Formatted: Left

Formatted: Left

Formatted: _Pld Footer Adjustment

given that AOSP's surreptitious mass-collection of Plaintiffs' data is unnecessary for and contrary to AOSP's stated function as a browser security extension, Plaintiffs would have no reason to investigate the possible interception, collection, storage, use, and sharing of their data by AOSP and Defendants. Second, Plaintiffs would have to have special expertise in identifying and interpreting the underlying html coding and the operation of AOSP in order to discover Defendants' wrongful conduct. But Plaintiffs lack this special expertise.

167. Specifically, Plaintiffs did not know and could not have known about the critical facts giving rise to their claims until, at the very earliest, when they first consulted with counsel. For Plaintiffs Lau and Karwowski, that was no earlier than September 2022. For Plaintiff Halim, that was no earlier than January 2023. For Plaintiff Klein, that was no earlier than April 2023. For Plaintiff McBride, that was no earlier than June 2023.

168. Plaintiffs acted with reasonable diligence to discover the facts giving rise to their claims and were unable to have made earlier discovery despite such diligence. Defendants not only marketed their software under the name "Avast Online ***Security & Privacy***," but aggressively touted it as allowing consumers to "[b]rowse with more privacy," "[b]lock online trackers," and "keep . . . online activities private and anonymous."[72] Defendants went as far as to claim that AOSP would "stop web companies from collecting and selling your personal data."[73] And when Defendants' conduct began to attract media scrutiny in January 2020, they furthered their misinformation campaign by apologizing and claiming that they would shutter Jumpshot and change their behavior.

169. Before consulting with counsel, Plaintiffs had no notice that Defendants continued to secretly harvest data even after shuttering Jumpshot and issuing apologetic statements, as no other reports or disclosures of this kind had been made. In the face of Defendants' repeated misrepresentations, prior to consulting with counsel, Plaintiffs and other ordinary users would not have reasonably suspected a software named "Avast Online ***Security & Privacy***," and marketed as

[72] Avast, *Online Security & Privacy*, https://www.avast.com/avast-online-security#mac (last visited Oct. 11, 2023).

[73] *Id.*

Formatted: _Pld Footer Adjustment

a solution for preventing online tracking, was itself secretly harvesting their data.

170. Upon learning about counsel's investigation into Defendants' improper interception, collection, storage, use, and sharing of AOSP users' personal data, Plaintiffs diligently sought to uncover the facts, including by consulting with, and hiring, knowledgeable counsel to bring this case.

171. Plaintiffs are not bringing any claims arising out of Defendants' affirmative statements that concealed Defendants' wrongful interception, collection, storage, use, and sharing of Plaintiffs' data. As such, the affirmative acts of concealment are wholly separate from the wrongful conduct underlying Plaintiffs' claims.

~~81.~~172. All statutes of limitations applicable to Plaintiffs' claims are also tolled as a result of Gen Digital and Avast's knowing and active concealment of their conduct alleged herein.

~~82.~~173. Among other things, as set forth above, Gen Digital and Avast made misleading statements, including in the very titles of the ~~extensions~~extension ("Online Security and Privacy~~" and "SafePrice~~"), and after a January 2020 investigation revealed Avast had been harvesting user data for sale to third parties ("the Jumpshot investigation"), Gen Digital and Avast intentionally concealed the true nature of their ongoing user data interception, collection, storage, use, and sharing practices.

174. Avast also actively misrepresented its conduct in January 2020, when it announced that it would wind down Jumpshot and cease its illicit collection and misuse of private data. Specifically, in a press release announcing the closure of Jumpshot, Avast CEO Ondrej Vlcek attempted to lull the public into a false sense of security by claiming that "***Avast's core mission is to keep its users safe online and to give users control over their privacy*** . . . The bottom line is that any practices that jeopardize user trust are unacceptable to Avast. We are vigilant about our users' privacy[.]" Vlcek repeated Avast's purported commitment to user privacy again later in the press release, representing that "Avast is focused on innovating to enhance our products ***for the benefit of our users and the protection of their privacy.***"[74]

[74] Press Release, Avast, *Avast to Commence Wind Down of Subsidiary Jumpshot*, (Jan. 30, 2020), https://press.avast.com/avast-to-commence-wind-down-of-subsidiary-jumpshot.

Formatted: Left

Formatted: _Pld Footer Adjustment

175. This statement was false, and Avast knew it. In reality, Avast had no intention of protecting the privacy of its users. Although Jumpshot was shuttered, Avast's illicit collection and misuse of private data continued, as described in more detail *supra*.

176. Avast's misrepresentation regarding the true nature of their software continues even today. Avast's website for AOSP (now rebranded as "Avast Premium Security") advertises it as a tool to "[p]rotect your privacy and personal data" and "block web spies." The ironic reality is that AOSP itself is an insidious "web spy" that is illicitly intercepting, collecting, storing, using, and sharing every click, every search, and every website that its users visit.[75]

~~83.~~177. Given Avast's numerous misrepresentations regarding the core nature of their activities, it is unsurprising that Plaintiffs ~~and Class and Subclass members~~ were ignorant of the information essential to pursue their claims~~,~~ without any fault or lack of diligence on their own part~~.~~ until they consulted with counsel.

178. Because of Gen Digital~~, Avast, and Jumpshot~~ and Avast's fraudulent and active concealment, including ongoing efforts to present themselves as champions of online safety and user privacy, Plaintiffs could not have reasonably uncovered Defendants' wrongdoing until they consulted with counsel.

~~84.~~179. Defendants were under a duty to disclose the true character, quality, and nature of their ~~activities to Plaintiffs and the~~ data interception, collection, storage, use, and sharing practices to Plaintiffs and the Class and Subclass members because (i) this is nonpublic information over which Defendants have exclusive control, (ii) Defendants know this information is not readily available to Plaintiffs and other ordinary users who lack the sophisticated expertise to discover the wrongdoing, and (iii) this information is highly relevant to such people in deciding whether to install and use AOSP. Based on this knowledge, Defendants purposefully and knowingly omitted information regarding the true character, quality, and nature of their interception, collection, storage, use, and sharing of Plaintiffs' and Class and Subclass ~~members. Gen Digital, Avast, and Jumpshot therefore are estopped from relying on any statute of~~

[75] Avast, *Avast Premium Security*, https://www.avast.com/en-us/premium-security#pc (last visited Oct. 11, 2023).

Formatted: Left

Formatted: Left

Formatted: _Pld Footer Adjustment

~~limitations.~~members' data.

180. Further, Plaintiffs had no reason to suspect that AOSP and Defendants were intercepting, collecting, storing, using, and sharing their data to this extent – including the persistent interception, collection, and storage of full-string URLs – given that such behavior is unnecessary and in fact contrary to the stated functionality of AOSP, as discussed in more detail *supra*.

~~85.~~181. All applicable statutes of ~~limitation also~~ limitations have been tolled by ~~operation of the discovery rule. Specifically, Plaintiffs and other Class and Subclass members could not have learned through the exercise of reasonable diligence of Gen Digital, Avast, and Jumpshot's conduct as~~ Defendants' knowledge and active concealment of their wrongful conduct alleged herein, which behavior is ongoing.

~~86.~~182. ~~Gen Digital, Avast, and Jumpshot's~~Defendants' fraudulent concealment and omissions are common to Plaintiffs and the Class and Subclass members.

CLASS ACTION ALLEGATIONS

~~87.~~183. Plaintiffs incorporate by reference all of the foregoing allegations.

~~88.~~184. Plaintiffs bring this lawsuit pursuant to Rules 23(b)(2) and (3) of the Federal Rules of Civil Procedure.

~~89.~~185. Plaintiffs seek to represent the following Classes and Subclasses, which are all subsumed within the original Class and Subclass in the original complaint:

> **First Nationwide Class:** All natural persons residing in the United States who used a web browser with the Avast Online Security & Privacy ~~and/or Avast SafePrice~~ browser extension installed and who had their private data, other than PHI, intercepted and/or collected via that extension.
>
> **First California Subclass:** All natural persons residing in California who used a web browser with the Avast Online Security & Privacy and~~/or Avast SafePrice~~ browser extension installed and who had their private data, other than PHI, intercepted and/or collected via that extension.
>
> **Second Nationwide Class**: All natural persons residing in the United States who used a web browser with the Avast Online Security & Privacy browser extension installed, and had their PHI intercepted and/or collected via that extension.

Formatted: Left

Formatted: Left

Formatted: Font: Not Bold

Formatted: _Pld Footer Adjustment

Second California Subclass: All natural persons residing in California who used a web browser with the Avast Online Security & Privacy browser extension installed, and had their PHI intercepted and/or collected via that extension.

~~90.~~186. Excluded from the ~~Class~~Classes and ~~Subclass~~Subclasses are Defendants, their current employees, co-conspirators, officers, directors, legal representatives, heirs, successors and wholly or partly owned subsidiaries or affiliated companies, and the Judge and court staff to whom this case is assigned.

~~91.~~187. The ~~Class~~Classes and ~~Subclass~~Subclasses and their counsel satisfy the prerequisites of Federal Rule of Civil Procedure 23(a) and 23(g) and the requirements of rule 23(b)(3).

i. Numerosity and Ascertainability:

~~92.~~188. Plaintiffs do not know the exact size of the Class or Subclass or the identities of their members. Such information is known to Defendants. At minimum, each Class and Subclass has many thousands of members. Reports indicate that AOSP ~~and SafePrice have~~has each been installed more than 10 million times from the Chrome Web Store. Reports indicate that AOSP has been installed more than 1 million times from the Edge Add-ons store~~ and SafePrice has been installed more than 600,000 times from the Edge Add-ons store.~~. Thus, the number of members in ~~the~~each Class and Subclass is so numerous that joinder of all Class or Subclass members is impracticable. Membership of the ~~Class~~Classes and ~~Subclass~~Subclasses is defined using objective criteria and individual members will be identifiable from Defendants' records.

ii. Commonality and Predominance:

~~93.~~189. Common questions of law and fact exist as to all ~~members of the~~ Class and Subclass members and predominate over questions affecting only individual members of the ~~Class~~Classes and ~~Subclass~~Subclasses, including the following:

a. Whether ~~Gen Digital and Avast~~Defendants intercepted, ~~received, and/or~~ collected, stored, used, and shared electronic communications of user information, detailed URL requests, webpage browsing ~~history,~~histories and search ~~history, and/or web activity~~queries, full string URLs containing the specific search term(s)

Formatted: Left

Formatted: Left

Formatted: Font color: Auto

Formatted: Left

Formatted: Font color: Text 1

Formatted: Font color: Text 1

Formatted: _Pld Footer Adjustment

communicated to the search engine, email inbox search queries, video viewing histories, and PHI from Plaintiffs and Class and Subclass members during the class period;

b. Whether ~~Gen Digital~~AOSP's surreptitious interception, collection, and ~~Avast~~storage of Plaintiffs' and Class and Subclass members' private data is unnecessary for AOSP's stated function as a browser security extension;

~~b.~~c. Whether Defendants falsely represented to the public, including Plaintiffs and Class and Subclass members, that ~~it~~they would stop ~~its~~their admitted practice of intercepting, ~~receiving, and/or~~ collecting ~~electronic communications of user information, browsing history, search history, and web activity~~, storing, using, and sharing Plaintiffs' and Class and Subclass members' private data after the 2020 Jumpshot investigation;

~~c. Whether Gen Digital and Avast's practice of intercepting, receiving, and/or collecting electronic communications of user information, browsing history, search history, and/or web activity violates state and federal privacy laws;~~

~~d.~~ Whether ~~Gen Digital and Avast's practice of intercepting, receiving, and/or collecting electronic communications of user information, browsing history, search history, and/or web activity violates state and federal anti-wiretapping laws;~~

~~e. Whether Gen Digital and Avast's practice of intercepting, receiving, and/or collecting electronic communications of user information, browsing history, search history, and/or web activity violates any other state and federal tort laws;~~

~~f.~~d. ~~Whether Gen Digital and Avast~~Defendants omitted or concealed material facts from the public, including Plaintiffs and Class and Subclass members, about ~~its~~their practice of intercepting, ~~receiving, and/or~~ collecting ~~electronic communications of user information, browsing history, search history,~~, storing, using, and sharing Plaintiffs' and ~~/or web activity~~ Class and Subclass members' private data;

~~g.~~e. Whether ~~Gen Digital, Avast, and Jumpshot~~Defendants owe a duty to Plaintiffs and Class and Subclass members to disclose material facts about their practice of

Formatted: Left

Formatted: Font color: Text 1

Formatted: Left

Formatted: _Pld Footer Adjustment

intercepting, ~~receiving,~~ collecting, ~~and/or~~storing, using ~~electronic communications of user information, browsing history, search history,~~, and sharing Plaintiffs' and~~/or web activity~~ Class and Subclass members' private data;

f. ~~Whether Gen Digital, Avast, and Jumpshot's~~Whether Defendants' practice of intercepting, collecting, storing, using, and sharing of electronic communications of user information, detailed URL requests, webpage browsing histories and search queries, full string URLs containing the specific search term(s) communicated to the search engine, email inbox search queries, video viewing histories, and PHI violates state and federal privacy laws;

g. Whether Defendants' practice of intercepting, collecting, storing, using, and sharing of electronic communications of user information, detailed URL requests, webpage browsing histories and search queries, full string URLs containing the specific search term(s) communicated to the search engine, email inbox search queries, video viewing histories, and PHI violates state and federal anti-wiretapping laws;

h. Whether Defendants' practice of intercepting, collecting, storing, using, and sharing of electronic communications of user information, detailed URL requests, webpage browsing histories and search queries, full string URLs containing the specific search term(s) communicated to the search engine, email inbox search queries, video viewing histories, and PHI violates any other state and federal tort laws;

~~h.~~i. Whether Defendants' conduct described herein violates Plaintiffs' and Class and Subclass members' interest in precluding the dissemination or misuse of sensitive and confidential information ("informational privacy");

~~i.~~j. Whether ~~Gen Digital, Avast, and Jumpshot's~~Defendants' conduct described herein violates Plaintiffs' and Class and Subclass members' interest in making intimate personal decisions or conducting activities without observation, intrusion, or interference ("autonomy privacy");

Formatted: Left

Formatted: _Pld Footer Adjustment

~~j.~~k. Whether ~~Gen Digital, Avast, and Jumpshot~~Defendants improperly obtained and/or disclosed Plaintiffs' and Class and Subclass members' private data without authorization or in excess of any authorization;

~~k.~~l. Whether profits obtained by ~~Gen Digital, Avast, and Jumpshot~~Defendants through the sale of ~~information~~private data or sale of access to ~~information~~private data that they obtained from Plaintiffs and Class and Subclass members were unjustly obtained and should be disgorged;

~~l.~~m. Whether any profits or other value obtained by ~~Gen Digital, Avast, and Jumpshot~~Defendants through analysis, enrichment, and other use of ~~information~~private data from Plaintiffs and Class and Subclass members were unjustly obtained by ~~Gen Digital, Avast, and Jumpshot~~Defendants, and should be disgorged;

~~m.~~n. Whether Plaintiffs and Class and Subclass members sustained damages as a result of ~~Gen Digital, Avast, and Jumpshot's~~Defendants' conduct, and, if so, what is the appropriate measure of damages or restitution; and

~~n.~~o. Whether Plaintiffs and Class and Subclass members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein.

~~94.~~190. Gen Digital, Avast, and Jumpshot engaged in a common course of conduct giving rise to the legal rights sought to be enforced by this action. Furthermore, similar or identical questions of statutory and common law, as well as similar or identical injuries, are involved. Individual questions, if any, pale in comparison to the numerous common questions that predominate in this action.

iii. Typicality:

~~95.~~191. Plaintiffs' claims are typical of the claims of other Class and Subclass members because, among other things, all ~~members of the~~ Class and Subclass members were uniformly affected by Defendants' wrongful conduct in violation of federal and state laws as complained of herein.

Formatted: Left

Formatted: Left

Formatted: _Pld Footer Adjustment

iv. Adequacy of Representation:

~~96.~~192. Plaintiffs will fairly and adequately protect the interests of the Class and Subclass members. Plaintiffs have retained counsel experienced in complex class actions and data privacy litigation, and Plaintiffs intend to vigorously prosecute this case on behalf of the Class and Subclass members. Further, Plaintiffs have no interests that are antagonistic to the Class and Subclass~~—~~ members.

v. Superiority:

~~97.~~193. A class action is superior to individual litigation and all other available methods for the fair and efficient adjudication of this controversy. The damages suffered by individual ~~members of the~~ Class and Subclass members are relatively small compared to the burden and expense required to individually litigate claims against Defendants. It would thus be impossible for ~~members of the~~ Class and Subclass members, on an individual basis, to obtain effective redress for the wrongs committed against them.

~~98.~~194. Moreover, individualized litigation presents the potential for inconsistent or contradictory judgments, and increases the delay and expense presented by the complex legal and factual issues of the case to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

(Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510~~, *Et Seq*~~ *et seq*. Against Defendant Gen Digital)

~~99.~~195. Plaintiffs, individually and on behalf of the Class and Subclass members, incorporate the foregoing allegations as if fully set forth herein.

~~100.~~196. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, proscribes the intentional interception, disclosure, or use of the contents of any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

~~101.~~197. The statute provides a private right of action to "any person whose wire,

Formatted: Left

Formatted: Left

Formatted: Left

Formatted: _Pld Footer Adjustment

oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

~~102.~~198. The Federal Wiretap Act protects both the sending and receipt of electronic communications.

~~103.~~199. Plaintiffs and Class and Subclass members, as individuals, are persons within the meaning of 18 U.S.C. § 2510(6).

~~104.~~200. When Plaintiffs or Class and Subclass Members install the AOSP ~~or SafePrice extensions~~extension, Gen Digital and Avast intercept communications between Plaintiffs and Class and Subclass members, on the one hand, and the Internet search engines they use and websites that they visit, on the other. Gen Digital and Avast's interception of those communications is intentional. Gen Digital and Avast are sophisticated software companies that know ~~their products are~~AOSP is intercepting communications in these circumstances and have taken no remedial action.

~~105.~~201. Gen Digital and Avast's interception of the communications ~~is~~occurs while the Plaintiffs' and Class and Subclass members' communications are in transit and/or in the process of being sent or received to and from the Internet search engines and websites to which they navigate.

~~106.~~202. The Federal Wiretap Act defines "contents" as including "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). The communications intercepted by Gen Digital and Avast include "contents" of electronic communications exchanged between Plaintiffs and Class and Subclass members, on the one hand, and the Internet search engines and other websites to which they navigated, on the other, in the form of detailed URL requests, webpage browsing histories and search queries, full string URLs containing the specific search term(s) communicated to the search engine, ~~and~~ email inbox search queries~~.~~, video viewing histories, and PHI. Plaintiffs and Class and Subclass members sent communications to those Internet search engines and websites, and Plaintiffs and Class and Subclass members received communications in return from those Internet search engines and websites.

Formatted: _Pld Footer Adjustment

~~107.~~203. The transmission of data between Plaintiffs and Class and Subclass members, on the one hand, and the Internet search engines and websites with which they chose to exchange communications, on the other, constitutes the "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce." The transmitted data is therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

~~108.~~204. Gen Digital and Avast intercept the electronic communications while they are in transit by using software that automatically duplicates the communication between the user and the Internet search engine or website and sends the duplicated information to Gen Digital and Avast's servers.

~~109.~~205. The communications between the Plaintiffs and Class and Subclass members, on the one hand, and Internet search engines and websites, on the other, were simultaneous to, but separate from, the channel through which Gen Digital and Avast acquired the contents of those communications.

~~110.~~206. The following constitute "devices" as defined under § 2510(5) of the Act:

a. The web browsers of Plaintiffs and Class and Subclass members;

b. The personal computing devices of Plaintiffs and Class and Subclass members;

c. The computer codes and programs used by Gen Digital and Avast to effectuate the interception of the communications that are exchanged between Internet search engines and websites, on the one hand, and Plaintiffs and Class and Subclass members, on the other, while browsing the Internet on a web browser with the AOSP ~~and/or SafePrice extensions~~extension installed;

d. Gen Digital and Avast's servers;

e. The servers of websites and Internet search engines from which Gen Digital and Avast intercepted the communications sent or received by Plaintiffs and Class and Subclass members; and

f. The plan Gen Digital and Avast carried out to effectuate the interception of the

Formatted: _Pld Footer Adjustment

communications that are exchanged between Internet search engines or websites, on the one hand, and Plaintiffs and Class and Subclass members, on the other, while browsing the Internet on a web browser with the AOSP ~~and/or SafePrice extensions~~extension installed.

~~111.~~207. For purposes of this Complaint, Gen Digital and Avast are not "electronic communication service[s]," as defined in 18 U.S.C. § 2510(12), nor are Gen Digital and Avast Internet Service Providers.

~~112.~~208. Gen Digital and Avast's unlawful interception of electronic communications is not excused under 18 U.S.C. § 2511(2)(c) because Gen Digital and Avast are not parties to the communication and have not received prior consent from the website, ~~search engines, Plaintiffs, or Class or Subclass members to engage in such interception.~~Internet search engines, Plaintiffs, or Class or Subclass members to engage in such interception. Avast engages in "unknown duplication and communication of" Plaintiffs' full-string URLs and private data, which "do not exempt a defendant from liability under the party exemption." *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 608 (9th Cir. 2020). Plaintiffs could not have known that this duplication and communication of their browsing histories was occurring, given that such persistent interception, collection, and storage of full-string URLs and private data is unnecessary for performing the stated function of a browser security extension, as alleged in more detail *supra*. Further, AOSP and Defendants can – and do – use this private data for purposes other than the stated purpose of providing browser security, namely by providing the information to third-party advertisers through dozens of advertising cookies used by the AOSP software. *See Javier v. Assurance IQ, LLC*, 2023 WL 114225, at *4 (N.D. Cal. Jan. 5, 2023) (stating that the applicability of the party exception to an eavesdropper turns on whether that party "ha[s] the capability to use its record of the interaction for any other purpose than to furnish information [to a party.]")

~~113.~~209. Neither the Plaintiffs nor Class or Subclass members were aware that Gen Digital and Avast were intentionally intercepting communications between Plaintiffs and Class or Subclass members, on the one hand, and the Internet search engines and websites that they use on web browsers with the AOSP ~~and/or SafePrice extensions~~extension installed, on the other.

Formatted: _Pld Footer Adjustment

Likewise, the websites and Internet search engines that Plaintiffs and Class and Subclass members visited did not know of or consent to Gen Digital and Avast's interception of the details about visitors' access to and activities on ~~their~~such websites and Internet search engines.

~~114.~~210. For the violations set forth above and pursuant to 18 U.S.C. § 2520, Plaintiffs and ~~members of the~~ Class and Subclass members seek (1) appropriate preliminary and other equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and Class and Subclass members and any profits made by Defendants as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; (3) punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Gen Digital and Avast in the future; and (4) reasonable attorney's fees and other litigation costs reasonably incurred.

SECOND CAUSE OF ACTION

(Violation of the California Invasion of Privacy Act, California Penal Code §§ 630~~,~~ *et seq.* Against Defendant Gen Digital)

~~115.~~211. Plaintiffs, individually and on behalf of the Class and Subclass members, incorporate the foregoing allegations as if fully set forth herein.

~~116.~~212. The California Invasion of Privacy Act ("CIPA"), codified at Cal. Penal Code §§ 630 to 638, begins by providing its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

~~117.~~213. California Penal Code § 631(a) imposes liability upon:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning

Formatted: Left

Formatted: Left

Formatted: _Pld Footer Adjustment

> of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section . . . .

Section 631(a) applies to communications conducted over the Internet.

~~118.~~214. California Penal Code § 632(a) imposes liability upon:

> A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio . . ~~.~~..

~~119.~~215. Under both section 631(a) and section 632(a), the alleged violator must show it had the consent of all parties to a communication to avoid liability.

~~120.~~216. At all relevant times, Gen Digital and Avast's interceptions of the Plaintiffs' and Class and Subclass members' Internet communications in transit originating in or sent to California were and are without the authorization or consent of the Plaintiffs, the Class and Subclass Members, and the websites and Internet search engines with which they communicated. Gen Digital and Avast were not participants to the communications and the interceptions by Gen Digital and Avast in the aforementioned circumstances were and are unlawful and tortious.

~~121.~~217. Plaintiffs ~~and~~Lau, Karwowski, and McBride, and the Subclass members were in California during one or more of their ~~internet~~Internet usage sessions in which Defendants stole their data. ~~-~~Upon information and belief, each Plaintiff and Class member, even those located outside of California, during one or more of their interactions on the Internet during the applicable statute of limitations period, communicated with one or more entities based in California, and/or with one or more entities whose servers were located in California. Communications from the California web-based entities to Plaintiffs and Class members were sent from California. Communications to the California web-based entities from Plaintiffs and Class members were sent

Formatted: Left

Formatted: Left

Formatted: _Pld Footer Adjustment

to California.

~~122.~~218. Plaintiffs and Class and Subclass members did not consent to any of Gen Digital and Avast's actions in intercepting, reading, and/or learning the contents of their communications with ~~such California-based entities~~the websites and Internet search engines with which Plaintiffs and Class and Subclass members communicated.

~~123.~~219. Gen Digital and Avast's non-consensual interception of the Plaintiffs' and Class and Subclass members' Internet communications while they were using web browsers with the AOSP ~~and/or SafePrice~~ extension installed was designed to attempt to learn at least some meaning of the content in the ~~communication~~communications between Plaintiffs and Class and Subclass members, on the one hand, and the websites and Internet search engines to which they navigated, on the other.

~~124.~~220. The communications intercepted by Gen Digital and Avast include "contents" of electronic communications exchanged between Plaintiffs and Class and Subclass members, on the one hand, and the Internet search engines and other websites to which they navigated, on the other, in the form of detailed URL requests, webpage browsing histories and search queries, full string URLs containing the specific search term(s) communicated to the search engine, ~~and~~ email inbox search queries~~.~~, video viewing histories, and PHI. Plaintiffs and Class and Subclass members sent communications to those Internet search engines and websites, and Plaintiffs and Class and Subclass members received communications in return from those Internet search engines and websites.

~~125.~~221. The following items constitute "machine[s], instrument[s], or contrivance[s]" under § 631(a), and even if they did not, Gen Digital and Avast's deliberate and admittedly purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

a. The Plaintiffs' and Class and Subclass members' browsers;

b. The Plaintiffs' and Class and Subclass members' personal computing devices;

c. The computer codes and programs used by Gen Digital and Avast to effectuate the interception of communications exchanged between websites and Internet search

Formatted: _Pld Footer Adjustment

engines, on the one hand, and Plaintiffs and Class and Subclass members, on the other, while browsing the Internet on a web browser with the AOSP ~~and/or SafePrice extensions~~extension installed;

d. Gen Digital and Avast's servers;

e. The servers of websites and Internet search engines from which Gen Digital and Avast intercepted the Plaintiffs' and Class and Subclass members' communications; and

f. The plan Gen Digital and Avast carried out to effectuate the interception of the communications that are exchanged between websites and Internet search engines, on the one hand, and Plaintiffs and Class and Subclass members, on the other, while browsing the Internet on a web browser with the AOSP ~~and/or SafePrice extensions~~extension installed.

~~126.~~222. The data intercepted, collected, stored, used, and shared by Gen Digital and Avast constituted "confidential communications," as that term is used in § 632(a), because PHI is by definition confidential and because Plaintiffs and Class and Subclass members have an objectively reasonable expectation of privacy that their private browsing communications are not being intercepted or disseminated.

~~127.~~223. Plaintiffs and Class and Subclass members have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their ~~personally identifiable information.~~private data.

~~128.~~224. Pursuant to California Penal Code § 637.2, Plaintiffs and Class and Subclass members have been injured by the violations of California Penal Code §§ 631 and 632, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive and/or other equitable relief.

THIRD CAUSE OF ACTION

(Invasion of Privacy Under Article I, Section 1 of the California Constitution Against All Defendants)

~~129.~~225. Plaintiffs, individually and on behalf of the Class and Subclass members, incorporate the foregoing allegations as if fully set forth herein.

Formatted: Left

Formatted: _Pld Footer Adjustment

~~130.~~226. In 1972, California added a right of privacy to the list of enumerated inalienable rights in Article I, § 1 of its Constitution.

~~131.~~227. To plead invasion of privacy under the California Constitution, Plaintiffs must allege "that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is 'so serious . . . as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020), quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009).

~~132.~~228. Plaintiffs and Class and Subclass members have a legally protected privacy interest in:

a. precluding the interception, collection, storage, copying, dissemination and/or misuse of their sensitive, confidential ~~personally identifiable~~ information, including PHI; and

b. making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various Internet sites without having that information intercepted and transmitted to Defendants without their knowledge or consent.

~~133.~~229. ~~Based on the names of the products ("Online Security and Privacy" and "SafePrice"),~~ Plaintiffs and Class and Subclass members had a reasonable expectation of privacy in the ~~personally identifiable information~~ private data Defendants intercept, collect, store, use, and share without adequately notifying users~~.~~, considering that:

a. Defendants intercept, collect, store, use, and share an enormous amount of private data, including all data exchanged between Plaintiffs and Class and Subclass members, on the one hand, and the websites and Internet search engines to which they navigate, on the other hand, including detailed URL requests, webpage browsing histories and search queries, full string URLs containing the specific search term(s) communicated to the search engine, email inbox search queries,

Formatted: _Pld Footer Adjustment

video viewing histories, and PHI;

b. Defendants intercept, collect, store, use, and share highly sensitive data that no common-sense user would expect Defendants to intercept, collect, store, use, and share, and that Plaintiffs and Class and Subclass members never consented to; and

c. Defendants do not disclose the true nature of their ongoing user data interception, collection, storage, use, and sharing practices, or the extent of the information intercepted, collected, stored, used, and shared, allowing Defendants to intercept, collect, store, use, and share user information, detailed URL requests, webpage browsing histories and search queries, full string URLs containing the specific search term(s) communicated to the search engine, email inbox search queries, video viewing histories, and PHI in a manner undetectable by users.

d. The interception, collection, storage, use, and sharing of Plaintiffs' and Class and Subclass members' private data is unnecessary to AOSP's function as a browser security extension.

~~134.~~230. Defendants' actions constitute a serious invasion of privacy in that they are:

a. Invading a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices, including ~~web search and browsing histories;~~detailed URL requests, webpage browsing histories and search queries, full string URLs containing the specific search term(s) communicated to the search engine, email inbox search queries, video viewing histories, and PHI;

b. Violating several federal criminal laws, including the Electronic Communications Privacy Act;

c. Invading the privacy interests and rights of millions of Americans (including Plaintiffs and Class and Subclass members) without their consent;

d. Engaging in the unauthorized taking of valuable information from millions of Americans ~~through deceit;~~without their knowledge or consent and

e. Committing criminal acts against millions of Americans, which constitutes an

Formatted: Left

Formatted: _Pld Footer Adjustment

egregious breach of social norms that is highly offensive.

~~135.~~231. The surreptitious and unauthorized interception of the Internet communications of millions of Americans, who have taken active measures to ensure their privacy by installing ~~Gen Digital and Avast's extensions~~AOSP, constitutes an egregious breach of social norms that is highly offensive.

~~136.~~232. Defendants' intentional intrusion into Plaintiffs' and Class and Subclass members' Internet communications and their computing devices and web browsers is highly offensive to a reasonable person in that Defendants violated federal and state criminal and civil laws designed to protect individual privacy and guard against theft.

~~137.~~233. The secret and unauthorized taking of personally-identifiable information, including PHI, from millions of Americans ~~through deceit~~without their knowledge or consent is highly offensive behavior.

~~138.~~234. The secret and unauthorized monitoring of private Internet browsing is highly offensive behavior.

~~139.~~235. Wiretapping and surreptitious recording of communications is highly offensive behavior. It is even more highly offensive when such conduct involves PHI.

236. In sum, the secret and unauthorized interception, collection, storage, use, and sharing of Internet search engine keyword searches, search results, email inbox searches, browsing histories, video viewing histories, and PHI is highly offensive behavior.

237. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions.

~~140.~~238. Defendants lacked a legitimate business interest in intercepting and receiving private Internet communications between Plaintiffs and Class and Subclass members, on the one hand, and the Internet search engines and websites to which they navigated, on the other, without first obtaining the consent of Plaintiffs, Class and Subclass members, or the websites and Internet search engines.

~~141.~~239. Plaintiffs and Class and Subclass members have sustained, and will

Formatted: Left

Formatted: _Pld Footer Adjustment

continue to sustain, damages as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation and injunctive relief, as well as such other relief as the Court may deem just and proper.

FOURTH CAUSE OF ACTION

(Intrusion Upon Seclusion
Against All Defendants)

~~142.~~240. Plaintiffs, individually and on behalf of the Class and Subclass members, incorporate the foregoing allegations as if fully set forth herein.

~~143.~~241. A claim for intrusion upon seclusion requires (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

~~144.~~242. By intercepting the Internet communications of Plaintiffs and Class and Subclass members, Defendants intentionally intruded upon their solitude or seclusion.

~~145.~~243. Gen Digital and Avast intentionally intruded upon Plaintiffs' and Class and Subclass members' solitude, seclusion, and private affairs by intentionally designing their ~~extensions~~extension and programming code to surreptitiously intercept and retain the private ~~and personally-identifiable information~~data of Plaintiffs and Class and Subclass members. Gen Digital and Avast effectively place themselves in the middle of conversations to which they are not an authorized party. ~~-~~Jumpshot intentionally intruded upon Plaintiffs' and Class and Subclass members' solitude, seclusion, and private affairs by intentionally receiving and using this information, knowing how it had been obtained.

~~146.~~244. Defendants intercept these Internet communications without authority or consent from Plaintiffs, Class and Subclass members, or the websites and Internet search engines with which they communicate.

~~147.~~245. Defendants' intentional intrusion into Plaintiffs and Class and Subclass members' Internet communications, computing devices, and web browsers is highly offensive to a reasonable person in that such intrusions violate federal and state criminal and civil laws designed to protect individual privacy and guard against theft.

~~148.~~246. The secret and unauthorized taking of personally-identifiable information, including PHI, from millions of Americans ~~through deceit~~without their knowledge or consent is

Formatted: Left

Formatted: _Pld Footer Adjustment

highly offensive behavior.

~~149.~~247. The secret and unauthorized monitoring of private Internet browsing is highly offensive behavior.

~~150.~~248. Wiretapping and surreptitious recording of communications is highly offensive behavior. It is even more highly offensive when such conduct involves PHI.

249. In sum, the secret and unauthorized interception, collection, storage, use, and sharing of Internet search engine keyword searches, search results, email inbox searches, browsing histories, video viewing histories, and PHI is highly offensive behavior.

~~151.~~250. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions.

~~152.~~251. Plaintiffs and Class and Subclass members reasonably expected that their ~~personal~~private data, including PHI, would not be intercepted, collected, stored, ~~or~~ used, or shared by Defendants.

252. Plaintiffs and Class and Subclass members have been damaged by these intrusions, which have allowed Defendants to obtain profits that rightfully belong to Plaintiffs and Class and Subclass members. Plaintiffs and Class and Subclass members are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful intrusion into ~~of~~ their private Internet communications.

~~153.~~

FIFTH CAUSE OF ACTION

(Statutory Larceny, California Penal Code §§ 484 and 496 Against All Defendants)

~~154.~~253. Plaintiffs, individually and on behalf of the Class and Subclass members, incorporate the foregoing allegations as if fully set forth herein.

~~155.~~254. California Penal Code Section 496(a) imposes liability upon

> [e]very person who buys or receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or who conceals, sells, withholds, or aids in concealing, selling, or withholding any

Formatted: Left

Formatted: Left, Indent: Left: 0.5", No bullets or numbering

Formatted: Left

Formatted: _Pld Footer Adjustment

> property from the owner, knowing the property to be so stolen or obtained . . .

~~156.~~ California Penal Code Section ~~484, which defines "theft," states in pertinent part:~~

255. ~~Every~~496(c) provides that "[a]ny person who ~~shall feloniously steal, take, carry, lead, or drive away~~has been injured by a violation of subdivision (a) . . . may bring an action for three times the ~~personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.~~amount of actual damages, if any, sustained by the plaintiff, costs of suit, and reasonable attorney's fees."

~~157. Pursuant to section 484(a), those who defraud others of personal property "by . . . false . . . representation or pretense . . . [are] guilty of theft." Cal. Penal Code § 484.~~

256. Defendants acted in a manner constituting theft, in violation of § 496(a), by taking possession of property owned by Plaintiffs and Class and Subclass members, without Plaintiffs' and Class and Subclass members' or their agents' consent, intending to deprive Plaintiffs and Class and Subclass members and/or their agents of the property permanently or long enough to deprive them of a major portion of the value or enjoyment of the property, and moving Plaintiffs' and Class and Subclass members' property, however slightly, and keeping it for any period of time, however brief. *See* Judicial Council of California Criminal Jury Instruction 1800 Theft by Larceny (Pen. Code, § 484).

~~158.~~257. Under California law, Plaintiffs' and Class and Subclass members' personal information constitutes property that may be the subject of theft.

~~159. Gen Digital and Avast acted in a manner constituting theft, in violation of § 496(a), by making false or fraudulent representations or pretenses to defraud Plaintiffs and Class and Subclass members of their personally-identifiable information.~~

~~160. To induce Plaintiffs and Class and Subclass members to use Gen Digital and Avast~~

Formatted: Font color: Text 1

Formatted: _2.0sp 0.5", Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Tab after: 0.5" + Indent at: 0"

Formatted: Font color: Text 1

Formatted: Font color: Text 1

Formatted: Left

Formatted: _Pld Footer Adjustment

~~products—a necessary component of Gen Digital and Avast's scheme to steal its users' personal information. Gen Digital and Avast use misleading and false product names and advertising claims to (i) intentionally misrepresent that their products make it safer and more secure to browse the Internet and (ii) promise to keep Plaintiffs' and Class and Subclass members' online communications safe and secure from data harvesters. Gen Digital and Avast knowingly make these false representations with the intent that Plaintiffs and Class and Subclass members will rely on them as true and use Gen Digital and Avast's products. Choosing to install and use Gen Digital and Avast's products demonstrates Plaintiffs' and Class and Subclass Members' reliance on Gen Digital and Avast's false representations regarding the safety and security of their data.~~

258. ~~Despite Gen Digital and Avast's false guarantee to the contrary,~~ Defendants unlawfully take possession of Plaintiffs' and Class and Subclass members' personal information when they intercept, copy and store Plaintiffs' and Class and Subclass members' detailed URL requests, webpage browsing histories and search queries, full string URLs containing the specific search term(s) communicated to the search engine, email inbox search queries, video viewing histories, and PHI, which is intercepted, collected, stored, used, and shared using the AOSP extension.

259. Users of the AOSP extension, including Plaintiffs and Class and Subclass members, do not consent to the extraction and sale of their sensitive and valuable Internet browsing data, such as Internet search engine keyword searches, search results, email inbox searches, browsing histories, video viewing histories, and PHI.

260. Defendants received, sold, or aided in selling, concealing, or withholding Plaintiffs' and Class and Subclass members' personal information with the intent to deprive Plaintiffs and Class and Subclass members of such personal information permanently or to deprive them of a major portion of the value or enjoyment of such property. Defendants demonstrated this intent by agreeing to wind down Jumpshot but never committing to delete the personal data they intercepted, collected, stored, used, and shared without the consent of their users or disgorge the profits they

Formatted: _Pld Footer Adjustment

garnered by virtue of such unauthorized conduct.[76]

~~161.~~261. Gen Digital and Avast knowingly harvested Plaintiffs' and Class and Subclass members' sensitive and valuable Internet browsing data~~,~~ (such as Internet search engine keyword searches, search results, email inbox searches, browsing histories, video viewing histories, and PHI), and sold their data for a profit, without Plaintiffs' and Class and Subclass members' knowledge or consent, and without compensating them.

~~162.~~262. ~~Gen Digital and Avast~~Defendants further violated section 496(a) by receiving, selling, or aiding in selling, concealing, or withholding Plaintiffs' and Class and Subclass members' personal information, knowing that such property was stolen or wrongfully obtained.

~~163.~~263. ~~Gen Digital and Avast~~Defendants knew at the time they received, sold, or aided in selling, concealing, or withholding Plaintiffs' and Class and Subclass members' personal information, that such property was stolen or wrongfully obtained. For example, Gen Digital and Avast's knowledge of this unlawful conduct was evidenced in January 2020, when Avast CEO, Ondrej Vlcek, conceded that "Avast's sale of user data through its subsidiary Jumpshot . . . rightfully raised a number of questions–including the fundamental question of trust."

~~164. Gen Digital and Avast received, sold, or aided in selling, concealing, or withholding Plaintiffs' and Class and Subclass members' personal information with the intent to deprive Plaintiffs and Class and Subclass members of such personal information permanently or to deprive them of a major portion of the value or enjoyment of such property. Gen Digital and Avast~~

[76] *See Avast PLC Full Year Results for the Year Ended 31 December 2021*, BLOOMBERG (Feb. 25, 2022), https://www.bloomberg.com/press-releases/2022-02-25/avast-plc-full-year-results-for-the-year-ended-31-december-2021 ("In January 2020 Avast decided to terminate the provision of anonymized data to its data analytics business, Jumpshot, having concluded that the business was not consistent long term with the Group's privacy priorities as a global cybersecurity company. As the company is also exiting its toolbar-related search distribution business (which had previously been an important contributor to AVG's revenues) and the browser clean-up business, the growth figures exclude all of these (referred to above and throughout the report as "Discontinued Business"), which are negligible. The Discontinued Business does not represent a discontinued operation as defined by IFRS 5 since it either has not been disposed of but rather it is being continuously scaled down or it is considered to be neither a separate major line of business, nor geographical area of operations.").

Formatted: Left

Formatted: _Pld Footer Adjustment

~~demonstrated this intent by agreeing to wind down Jumpshot but never committing to delete the personal data they collected and shared without the consent of their users or disgorge the profits they garnered by virtue of such unauthorized conduct.~~

~~165.~~264. Jumpshot violated California Penal Code § 496(a) by buying or receiving Plaintiffs' and Class and Subclass members' personal information that Gen Digital and Avast had stolen or obtained in a manner constituting theft, knowing the property to be so stolen or obtained.

~~166.~~265. Jumpshot further violated § 496(a) by concealing, selling, or withholding, or aiding in concealing, selling, or withholding Plaintiffs' and Class and Subclass members' personal information that Gen Digital and Avast had stolen or obtained in a manner constituting theft, knowing the property to be so stolen or obtained.

~~167.~~266. Plaintiffs and Class and Subclass members' personal data carries tremendous financial value, as evinced by the tens of millions in annual ~~revenue~~revenues generated by Gen Digital and Avast licensing their users' data to Jumpshot. Further substantiating the economic value of this personal data, in December 2018, a major marketing provider paid Jumpshot $6.5 million for a three-year supply of the daily click-stream data generated by Gen Digital and Avast users.

~~168.~~267. Plaintiffs and Class and Subclass members did not consent to the extraction and sale of their detailed Internet browsing data~~,~~ (such as Internet search engine keyword searches, search results, email inbox searches, browsing histories, video viewing histories, and PHI), nor did they have any control over its use to produce revenue; therefore, Defendants' profits on such personal data were unjustly earned.

~~169.~~268. Plaintiffs and Class and Subclass members retain a stake in the unjustly earned profits Defendants derived from their violations of California Penal Code § 496(a).

~~170.~~269. While the exact value of Plaintiffs' and Class and Subclass members' personal information in this action will be a matter for expert determination, it is clear that Defendants have been unjustly enriched by the practices described herein and Plaintiffs and Class and Subclass members have a right to disgorgement and/or restitution damages for the value of their stolen data.

Formatted: Left

Formatted: _Pld Footer Adjustment

~~171.~~270. Pursuant to Penal Code § 496(c), Plaintiffs and Class and Subclass members are entitled to treble damages, as well as attorneys' fees and costs, for injuries sustained as a result of Defendants' violations of § 496(a).

SIXTH CAUSE OF ACTION

(Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200~~,~~ *et seq.* Against All Defendants)

~~172.~~271. Plaintiffs, individually and on behalf of the Class and Subclass members, incorporate the foregoing allegations as if fully set forth herein.

~~173.~~272. The California Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200. Defendants have violated the UCL.

~~174.~~273. Defendants' "unlawful" acts and practices include:

a. Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.* (Gen Digital and Avast);

b. Violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 631 and 632 (Gen Digital and Avast);

c. Invasion of Privacy under Article I, § 1 of the California Constitution (All Defendants);

d. Intrusion Upon Seclusion (All Defendants);

e. Statutory Larceny, California Penal Code §§ 484 and 496 (All Defendants).

~~175.~~274. All Defendants violated the "unlawful" prong of the UCL through their violation of statutes, Constitutional provisions, and common law, as alleged above.

~~176.~~275. All Defendants violated the "unfair" prong of the UCL because they intercepted communications, or knowingly received intercepted communications, containing the private ~~and personally-identifiable information~~data of Plaintiffs and Class and Subclass members (detailed URL requests, webpage browsing histories and search queries, full string URLs containing the specific search term(s) communicated to the search engine, email inbox search queries, video viewing histories, and PHI) under circumstances in which Plaintiffs and Class and

Formatted: Left

Formatted: _Pld Footer Adjustment

Subclass members would have no reason to know that such information was being intercepted because it was never disclosed or otherwise made known to them by Defendants. To establish liability under the unfair prong, Plaintiffs and Class and Subclass members need not establish that these statutes were actually violated, although the claims pleaded herein do so.

~~177.~~276. ~~All~~ Defendants also violated the "unfair" prong of the UCL because their business acts and practices are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of the harm posed and caused by Defendants secretly intercepting, collecting ~~or receiving~~, storing, using, and sharing private data about Plaintiffs and the Class and Subclass members is significant, and there is no corresponding benefit resulting from such conduct. Because Plaintiffs and the Class and Subclass members were ~~completely~~ unaware of Defendants' conduct, they could not have avoided the harm.

~~178.~~277. Plaintiffs and Class and Subclass members have suffered injury-in-fact, including the loss of money and/or property as a result of ~~Defendants~~Defendants' unfair and/or unlawful practices, to wit, the unauthorized interception, collection, storage, use, and sharing of their personal information which has value in an amount to be proven at trial. Moreover, Plaintiffs and Class and Subclass members have suffered harm in the form of diminution of the value of their private ~~and personally-identifiable data and content.~~ data.

~~179.~~278. Defendants' actions caused damage to and loss of Plaintiffs' and Class and Subclass members' property right to control the dissemination and use of their personal information and communications.

~~180.~~279. Defendants have taken property from Plaintiffs and the Class and Subclass members without providing just, or any, compensation.

~~181.~~280. Defendants should be required to cease their unfair and/or illegal interception, collection ~~of~~, storage, use, and sharing of private user data and to retrieve and delete all unfairly and/or illegally obtained private user data.

~~182.~~281. Defendants reaped unjust profits and revenues in violation of the UCL. Plaintiffs and Class and Subclass members seek injunctive relief governing Defendants' ongoing taking and possession of their information, or failure to account to Plaintiffs, ~~the~~ and Class and ~~the~~

Formatted: _Pld Footer Adjustment

Subclass members concerning ~~their~~Defendants' possession and use of ~~their~~Plaintiffs' and Class and Subclass members' data, and restitution and disgorgement of these unjust profits and revenues.

~~183.~~282. Plaintiffs~~, the~~ and Class~~,~~ and ~~the~~ Subclass members lack an adequate remedy at law because the ongoing harms from Defendants' taking, possession, and use of data must be addressed by injunctive relief and, due to the ongoing ~~and~~ nature of the harm, cannot be adequately addressed by monetary damages alone.

SEVENTH CAUSE OF ACTION

(Unjust Enrichment
Against All Defendants)

~~184.~~283. Plaintiffs, individually and on behalf of the Class and Subclass members, incorporate the foregoing allegations as if fully set forth herein.

~~185.~~284. Plaintiffs and Class and Subclass members conferred a benefit on Defendants in the form of highly personal ~~web browsing data~~data (detailed URL requests, webpage browsing histories and search queries, full string URLs containing the specific search term(s) communicated to the search engine, email inbox search queries, video viewing histories, and PHI) which has substantial monetary value that Defendants extracted and used to produce revenue and unjustly retained those benefits at the expense of Plaintiffs and Class and Subclass members.

~~186.~~285. Defendants intercepted, collected, stored, licensed, packaged ~~and/or~~, used, and shared this information for their own gain, reaping economic, intangible, and other benefits, including substantial monetary compensation from those who purchase or obtain access to Plaintiffs' and Class and Subclass members' ~~personal web browsing~~private data.

~~187.~~286. Defendants unjustly retained those benefits at the expense of Plaintiffs and Class and Subclass members because Defendants' conduct damaged Plaintiffs and Class and Subclass members, all without providing any commensurate compensation to Plaintiffs and Class and Subclass members.

~~188.~~287. Plaintiffs and Class and Subclass members did not consent to the extraction

Formatted: Left

Formatted: _Pld Footer Adjustment

and sale of their detailed Internet browsing data~~.~~ (such as Internet search engine keyword searches, search results, email inbox searches, browsing histories, video viewing histories, and PHI), nor did they have any control over its use to produce revenue. Therefore, under principles of equity and good conscience, Defendants should not be permitted to retain any money derived from their provision, licensing, or sale of information to Jumpshot or any third party, and Defendant Jumpshot should not be permitted to retain any money derived from its receipt or sale of Plaintiffs' and Class and Subclass members' personal Internet browsing data.

~~189.~~288. The benefits that Defendants derived from Plaintiffs and Class and Subclass members rightly belong to Plaintiffs and Class and Subclass members. It would be inequitable under unjust enrichment principles to permit Defendants' retention of any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request relief against Defendants as set forth below:

a. entry of an order certifying the proposed class and subclass pursuant to Federal Rule of Civil Procedure 23;

b. entry of an order appointing Plaintiffs as ~~representative~~representatives of the ~~Class~~Classes and ~~Subclass~~Subclasses;

c. entry of an order appointing Plaintiffs' counsel as co-lead counsel for the ~~Class~~Classes and ~~Subclass~~Subclasses;

d. entry of an order for injunctive and declaratory relief as described herein, including but not limited to:

i. enjoining Defendants from continuing to intercept, ~~receive, and/or~~ collect, store, use, and share electronic communications of user information, detailed URL requests, webpage browsing ~~history,~~histories and search ~~history, and/or web activity~~queries, full string URLs containing the specific search term(s) communicated to the search engine, email inbox search queries, video viewing histories, and PHI;

Formatted: Left

Formatted: Font color: Text 1

Formatted: Font color: Text 1

Formatted: _Pld Footer Adjustment

ii. enjoining Defendants from transmitting any additional user data to any person or entity;

iii. enjoining Defendants from taking and transmitting to anyone else the above-described user data;

iv. requiring Defendants to provide Plaintiffs with credit monitoring services;

v. requiring Defendants to return or destroy any and all data that was sold by Defendants;

vi. requiring Defendants to destroy the user data taken pursuant to the above practices, including that user data in the possession of third parties;

vii. requiring Defendants to provide confirmation that the above steps have been implemented;

viii. requiring Defendants to provide each consumer whose information was unlawfully intercepted, collected, stored, used, and/or shared with notice of who that information was communicated to;

e. entry of judgment in favor of each Class and Subclass member for damages suffered as a result of the conduct alleged herein, punitive damages, restitution, and disgorgement, to include interest and prejudgment interest;

f. leave to amend this Complaint to conform to the evidence produced at trial;

g. award Plaintiffs and Class and Subclass members their reasonable costs and expenses incurred in this action, including attorneys' fees and costs; and

h. grant such other and further legal and equitable relief as the court deems just and equitable.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Formatted: Left

Formatted: _Pld Footer Adjustment

DATED: February 28, 2024

Ekwan E. Rhow
Marc E. Masters
~~Oliver Rocos~~
~~BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW~~Bird, Marella, Boxer, Wolpert, Nessim, Drooks, Lincenberg & Rhow, P.C.

By: */s/ Ekwan E. Rhow*

Attorneys for Plaintiffs

Formatted: Font: Not Italic

DATED: February 28, 2024

Jonathan M. Rotter
David J. Stone
~~GLANCY PRONGAY & MURRAY~~Glancy Prongay & Murray LLP

By: */s/ Jonathan M. Rotter*

Attorneys for Plaintiffs

Formatted: Font: Not Italic

DATED: February 28, 2024

Korey A. Nelson
Amanda K. Klevorn
Claire E. Bosarge
~~BURNS CHAREST~~Burns Charest LLP

By: */s/ Korey A. Nelson*

Attorneys for Plaintiffs

Formatted: Font: Not Italic

~~Pursuant to Civil L.R. 5-1(h)(3), all signatories concur in filing this stipulation.~~

~~Dated: December 19, 2022~~ ~~*s/ Jonathan M. Rotter*~~
~~Jonathan M. Rotter~~

Formatted: Indent: Left: 0"

Formatted: _Pld Footer Adjustment